# Microsoft Solutions for Security and Compliance

# Windows XP Security Guide

Microsoft

# Contents

# Feedback

The Microsoft Solutions for Security and Compliance team would appreciate your thoughts about this and other security solutions.

Have an opinion? Let us know on the Security Solutions Blog for the IT Professional at http://blogs.technet.com/secguide.

Or e-mail your feedback to the following address: secwish@microsoft.com.

We look forward to hearing from you.

# Chapter 1: Introduction to the Windows XP Security Guide

## Overview

Welcome to the *Windows XP Security Guide*. This guide is designed to provide you with the best information available to assess and counter security risks that are specific to Microsoft® Windows® XP Professional with Service Pack 2 (SP2) in your environment. The chapters in this guide provide detailed information about how to configure enhanced security settings and features in Windows XP wherever possible to address identified threats in your environment. If you are a consultant, designer, or systems engineer who works in a Windows XP environment, this guide was designed with you in mind.

Microsoft engineering teams, consultants, support engineers, partners, and customers have reviewed and approved the information in this guide to make it:

- **Proven**. Based on field experience.
- **Authoritative**. Offers the best advice available.
- **Accurate**. Technically validated and tested.
- **Actionable**. Provides the steps to success.
- **Relevant**. Addresses real-world security concerns.

Best practices to secure both client and server computers were developed by consultants and systems engineers who have implemented Windows XP Professional, Microsoft Windows Server™ 2003, and Windows 2000 in a variety of environments, and these best practices are detailed in this guide. Step-by-step security prescriptions, procedures, and recommendations are also provided to help you maximize security for computers in your organization that run Windows XP Professional with SP2.

If you want more in-depth discussion of the concepts behind this material, see *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, the *Microsoft Windows XP Resource Kit*, the *Microsoft Windows Server 2003 Resource Kit*, the *Microsoft Windows Security Resource Kit*, and Microsoft TechNet.

This guide was originally created for Windows XP with SP1. This updated version reflects the significant security enhancements that Windows XP with SP2 provides, and it was developed and tested with computers that run Windows XP Professional with SP2. All references to Windows XP that are made in this guide refer to Windows XP with SP2 unless otherwise stated.

## Executive Summary

Whatever your environment, you are strongly advised to be serious about security matters. Many organizations underestimate the value of their information technology (IT) environment, often because they exclude substantial indirect costs. If an attack on the servers in your environment is severe enough, it could significantly damage the entire organization. For example, an attack that makes your Web site unavailable and causes a major loss of revenue or customer confidence

might lead to the collapse of your organization's profitability. When you evaluate security costs, you should include the indirect costs that are associated with any attack in addition to the costs of lost IT functionality.

Vulnerability, risk, and exposure analysis with regard to security informs you of the tradeoffs between security and usability that all computer systems are subject to in a networked environment. This guide documents the major security-related countermeasures that are available in Windows XP with SP2, the vulnerabilities that they address, and the potential negative consequences (if any) of each countermeasure's implementation.

The guide then provides specific recommendations for hardening computers that run Windows XP with SP2 in three common environments:

- **Enterprise Client (EC)**. Client computers in this environment are located in an Active Directory® directory service domain and only need to communicate with systems running Windows 2000 or later versions of the Windows operating system.
- **Stand-alone (SA)**. Client computers in this environment are not members of an Active Directory domain and may need to communicate with systems that run Windows NT® 4.0.
- **Specialized Security – Limited Functionality (SSLF)**. Concern for security in this environment is so great that a significant loss of functionality and manageability is acceptable. For example, military and intelligence agency computers operate in this type of environment.

This guide is organized for easy accessibility so that you can quickly find the information you need to determine what settings are suitable for your organization's computers that run Windows XP with SP2. Although this guide was designed for the enterprise customer, much of it is appropriate for organizations of any size.

To obtain the most value from this material, you will need to read the entire guide. The team that produced this guide hopes that you will find the material covered in it useful, informative, and interesting. For further information, you can also refer to the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available for download at http://go.microsoft.com/fwlink/?LinkId=15159.

# Who Should Read This Guide

This guide is primarily intended for consultants, security specialists, systems architects, and IT professionals who plan application or infrastructure development and the deployment of Windows XP workstations in an enterprise environment. This guide is not intended for home users. This guide is designed for individuals whose job roles include the following:

- System architects and planners who drive the architecture efforts for computers in their organizations.
- IT security specialists who focus on how to provide security across computing platforms within an organization.
- Business analysts and business decision makers (BDMs) who have critical business objectives and requirements that need IT desktop or laptop support.
- Consultants from both Microsoft Services and partners who need knowledge transfer tools for enterprise customers and partners.

## Skills and Readiness

The following knowledge and skills are required for administrators and architects who develop, deploy, and secure Windows XP client computers in an enterprise organization.

- MCSE 2000 or later certification with more than two years of security-related experience or the equivalent.
- In-depth knowledge of the organization's domain and Active Directory environments.
- Use of management tools, including MMC, Secedit, Gpupdate, and Gpresult.
- Experience in the administration of Group Policy.
- Experience deploying applications and client computers in enterprise environments.

# Scope of this Guide

This guide focuses on how to create and maintain a secure environment for desktops and laptops that run Windows XP Professional with SP2. The guide explains the different stages of how to secure three different environments and what each setting addresses for desktop and laptop computers that are deployed in each one. Information is provided for Enterprise Client (EC), Stand-Alone (SA), and Specialized Security – Limited Functionality (SSLF) environments.

Settings that are not specifically recommended as part of this guide are not documented. For a thorough discussion of all the security settings in Windows XP, refer to the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP* at http://go.microsoft.com/fwlink/?LinkId=15159.

## Enterprise Client

The Enterprise Client (EC) environment consists of a Windows 2000 or Windows Server 2003 Active Directory domain. The client computers in this environment will be managed through Group Policy that is applied to sites, domains, and organizational units (OUs). Group Policy provides a centralized method to manage security policy across the environment.

## Stand-Alone Client

The Stand-Alone Client (SA) environment includes client computers that cannot be joined to a domain or computers that are members of a Windows NT 4.0 domain. These client computers have to be configured through local policy settings. The management of stand-alone computers can be a considerably greater challenge than management of user accounts and policies in an Active Directory–based domain.

## Specialized Security – Limited Functionality

The Specialized Security – Limited Functionality (SSLF) environment provides elevated security settings for client computers. When these security policy settings are applied, user functionality may be noticeably reduced because it is limited to only those specific functions that are required for the necessary tasks. Access is limited to approved applications, services, and infrastructure environments. To be clear, security policy settings for the SSLF environment only apply to a few systems at a very small number of organizations, such as military and intelligence agencies. These settings tend to favor security over manageability and usability; they should only be used on computers whose compromise could cause significant financial loss or loss of life. In other words, the SSLF settings are not a good choice for most organizations.

# Chapter Overview

Windows XP with SP2 provides the most dependable version of a Windows client operating system to date, with improved security and privacy features. Overall security has been improved in Windows XP to help ensure your organization can work in a safer and more secure computing environment. The *Windows XP Security Guide* consists of seven chapters, and chapters two through six discuss the procedures that are required to create such an environment. Each of these chapters builds on an end-to-end process that is designed to secure Windows XP–based computers.

## *Chapter 1: Introduction to the Windows XP Security Guide*

This chapter includes an overview of the guide, descriptions of the intended audience, the problems that are discussed in the guide, and the overall intent of the guide.

## *Chapter 2: Configuring the Active Directory Domain Infrastructure*

You can use Group Policy to manage user and computer environments in Windows Server 2003 and Windows 2000 domains. It is an essential tool for securing Windows XP, and can be used to apply and maintain a consistent Security policy across a network from a central location. This chapter discusses the preliminary steps that must be performed in your domain before you apply Group Policy to your Windows XP client computers.

Group Policy settings are stored in Group Policy objects (GPOs) on domain controllers. GPOs are linked to sites, domains, and OUs within the Active Directory structure. Because Group Policy is so closely integrated with Active Directory, it is important to have a basic understanding of your Active Directory structure and security implications before you implement Group Policy.

## *Chapter 3: Security Settings for Windows XP Clients*

This chapter describes the security settings for Windows XP client computers that may be set through Group Policy in a Windows 2000 or Windows Server 2003 Active Directory domain. Guidance is not provided for all of the available settings—only those settings that will help secure an environment from most current threats are provided. The guidance also allows users to continue to perform typical job functions on their computers. The settings that you configure should be based on your organization's security goals.

## *Chapter 4: Administrative Templates for Windows XP*

In this chapter, settings that can be added to Windows XP by using Administrative Templates are discussed. Administrative Templates are Unicode files that you can use to configure the registry–based settings that govern the behavior of many services, applications, and operating system components. There are many Administrative Templates that can be used with Windows XP, and they contain hundreds of settings.

## Chapter 5: Securing Stand-Alone Windows XP Clients

Although most of this guide focuses on the Enterprise Client (EC) and Specialized Security – Limited Functionality (SSLF) environments, this chapter also discusses the configuration of stand-alone Windows XP client computers. Microsoft recommends that Windows XP be deployed in an Active Directory domain infrastructure, but recognizes that it is not always possible to do so. This chapter provides guidance about how to apply the recommended configurations to Windows XP with SP2 client computers that are not members of a Windows 2000 or Windows Server 2003 domain.

## Chapter 6: Software Restriction Policy for Windows XP Clients

This chapter provides a basic overview of software restriction policy, which provides administrators with a policy-driven mechanism to identify and limit the software that can be run in their domain. Administrators can use a software restriction policy to prevent unwanted programs from running and prevent viruses, Trojan horses, or other malicious code from spreading. Software restriction policies fully integrate with Active Directory and Group Policy, and they can also be used in an environment without a Windows Server 2003 domain infrastructure when applied to only the local computer.

## Chapter 7: Conclusion

The final chapter reviews the important points of the guide in a brief overview of everything that is discussed in the previous chapters.

## Appendix A: Key Settings to Consider

Although this guide discusses many security countermeasures and security settings, it is important to understand a small number of them are especially important. This appendix discusses the settings that will have the biggest impact on the security of computers that run Windows XP with SP2.

## Appendix B: Testing the Windows XP Security Guide

This appendix explains how the *Windows XP Security Guide* was tested in a lab environment to ensure that the guidance works as expected.

# Download Content

A collection of security templates, scripts, and additional files is included with this guide to make it easier for your organization to evaluate, test, and implement the recommended countermeasures.

Security templates are text files that can be imported into domain–based Group Policies or applied locally with the Microsoft Management Console (MMC) Security Configuration and Analysis snap-in. Procedures that describe how to accomplish these tasks are detailed in Chapter 2, "Configuring the Active Directory Domain Infrastructure." You can use the scripts that are included with this guide to implement the recommended countermeasures on stand-alone workstations.

Also included in the download content is the Microsoft Excel® workbook "Windows XP Security Guide Settings," which documents the settings that are included in each of the security templates.

The files that accompany this guide are collectively referred to as tools and templates. These files are included in a .msi file within the self-extracting WinZip archive that contains this guide. The download version of the Windows XP Security Guide is available at http://go.microsoft.com/fwlink/?LinkId=14840. When you execute the .msi file, the following folder structure will be created in the location that you specify:

- **\Windows XP Security Guide Tools and Templates\Security Templates**. This folder contains all security templates that are discussed in Chapters 2 and 3 of the guide. It also contains an Excel spreadsheet that summarizes all of the recommendations in the guide.
- **\Windows XP Security Guide Tools and Templates\SCE Update**. This folder contains scripts and data files to automatically update the user interface for the Security Configuration Editor as discussed in Chapter 3 of the guide.
- **\Windows XP Security Guide Tools and Templates\Stand Alone Clients**. This folder contains all sample scripts and templates that are used to harden stand-alone computers, which are discussed in Chapter 5 of the guide.
- **\Windows XP Security Guide Tools and Templates\Test Tools**. This folder contains tools that are related to "Appendix B: Testing the Windows XP Security Guide."

# Style Conventions

This guide uses the following style conventions.

**Table 1.1 Style Conventions**

| Element | Meaning |
|---|---|
| **Bold font** | Signifies characters typed exactly as shown, including commands, switches and file names. User interface elements also appear in bold. |
| *Italic font* | Titles of books and other substantial publications appear in *italic*. |
| *<Italic>* | Placeholders set in italic and angle brackets *<filename>* represent variables. |
| `Monospace font` | Defines code and script samples. |
| **Note** | Alerts the reader to supplementary information. |
| Important | Alerts the reader to essential supplementary information. |

# Summary

This chapter introduced you to the *Windows XP Security Guide* and summarized the guide's chapters. When you understand how the guide is organized, you are ready to take full advantage of the key security options that are built into Windows XP with SP2.

Effective, successful security operations require effort in all of the areas that are discussed in this guide, not just improvements in one. For this reason, it is highly recommended that you implement the recommendations in this guide that are appropriate for your organization as part of a wider defense-in-depth security architecture.

# More Information

The following links provide additional information about Windows XP Professional security-related topics.

- For more information about security settings that can be configured on Microsoft Windows XP, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.
- For information about how to implement security on servers in a manner that is analogous to what is discussed in this guide, see the Windows Server 2003 Security Guide. The recommendations in this guide are designed to be applied to servers that need to support Windows XP client computers that are configured as described in the remaining chapters. It is available online at http://go.microsoft.com/fwlink/?LinkId=14845.
- For information about how to implement security risk management more effectively in your organization, see the Security Risk Management Guide at http://go.microsoft.com/fwlink/?LinkID=30794.
- For information about how to minimize the impact of malicious software, see The Antivirus Defense-in-Depth Guide at http://go.microsoft.com/fwlink/?LinkId=28732.
- For information about how to minimize the dependence on using passwords for authentication in your organization, see The Secure Access Using Smart Cards Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41313.
- For information about how to more effectively watch for and respond to potential security violations in your organization, see The Security Monitoring and Attack Detection Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41309.
- For more details about how the Microsoft Operations Framework (MOF) can assist you in your organization, see http://www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspx.
- For information about Microsoft Windows Security, see the Microsoft Security Home Page at http://www.microsoft.com/security/.
- For information about the Microsoft Technical Security Notifications service, see http://www.microsoft.com/technet/security/bulletin/notify.asp.

# Chapter 2: Configuring the Active Directory Domain Infrastructure

## Overview

Group Policy is a feature of the Active Directory® directory service that facilitates change and configuration management in Microsoft® Windows Server™ 2003 and Microsoft Windows® 2000 Server domains. However, you need to perform certain preliminary steps in your domain before you apply Group Policy to the Microsoft Windows XP Professional with Service Pack 2 (SP2) client computers in your environment.

Group Policy settings are stored in Group Policy objects (GPOs) in the Active Directory database. The GPOs are linked to containers, which include Active Directory sites, domains, and organizational units (OUs). Because Group Policy is so closely integrated with Active Directory, it is important to have a basic understanding of Active Directory structure and the security implications of different design configuration options within it before you implement Group Policy. For more information about Active Directory design, see Chapter 3, "The Domain Policy," of the *Windows Server 2003 Security Guide*.

Group Policy is an essential tool for securing Windows XP. This chapter provides details about how to use Group Policy to apply and maintain a consistent security policy across a network from a central location.

This guide presents options for both Enterprise Client (EC) and Specialized Security – Limited Functionality (SSLF) environments. The settings that are recommended in this chapter are identical for both desktop and laptop client computers, and because they are special-case settings they are applied at the domain root level instead of the OU level. For example, password and account lockout policies for Windows Server 2003 and Windows 2000 Server domains must be configured through a GPO that is linked to the domain root. The names of the baseline security template files for the two different environments are:

- EC-Domain.inf
- SSLF-Domain.inf

## OU Design to Support Security Management

An OU is a container within an Active Directory domain. An OU may contain users, groups, computers, and other OUs, which are known as child OUs. You can link a GPO to an OU, and the GPO settings will be applied to the users and computers that are contained within that OU and its child OUs. To facilitate administration you can delegate administrative authority to each OU. OUs provide an easy way to group users, computers, and other security principals, and they also provide an effective way to segment administrative boundaries. Microsoft recommends that organizations assign users and computers to separate OUs, because some settings only apply to users and other settings only apply to computers.

You can delegate control over a group or an individual OU by using the Delegation Wizard in the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in tool. See the “More Information” section at the end of this chapter for links to documentation about how to delegate authority.

One of the primary goals of an OU structure design for any environment is to provide a foundation for a seamless Group Policy implementation that applies to all workstations in Active Directory and ensures that they meet the security standards of your organization. The OU structure must also be designed to provide adequate security settings for specific types of users in an organization. For example, developers may be permitted to do things on their workstations that average users should not be allowed to do. Also, laptop users may have slightly different security requirements than desktop users. The following figure illustrates a simple OU structure that is sufficient for the Group Policy discussion in this chapter. The structure of this OU may differ from the organizational requirements of your environment.

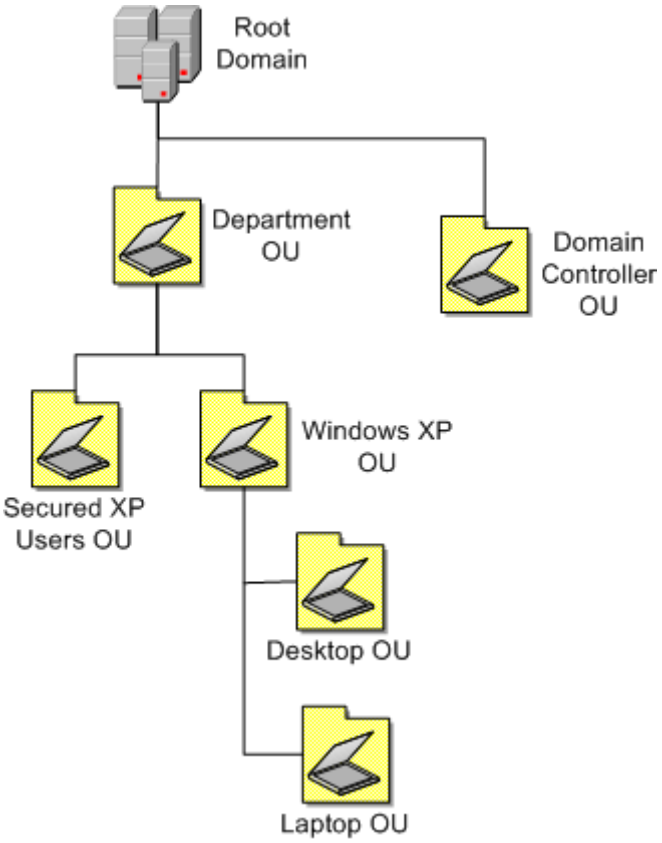


**Figure 2.1 An OU structure for Windows XP computers**

# *Department OU*

Because security requirements often vary within an organization, it may make sense to create department OUs in your environment. The departmental security settings can be applied through a GPO to the computers and users in their respective department OUs.

## Secured XP Users OU

This OU contains the accounts for users in both the EC and SSLF environments. The settings that are applied to this OU are discussed in the “User Configuration” section of Chapter 4, "Administrative Templates for Windows XP."

## Windows XP OU

This OU contains child OUs for each type of Windows XP client computer in your environment. Guidance is included in this guide for desktop and laptop computers. For this reason, a Desktop OU and a Laptop OU have been created.

- **Desktop OU**. This OU contains desktop computers that constantly remain connected to your network. The settings that are applied to this OU are discussed in detail in Chapter 3, "Security Settings for Windows XP Clients," and Chapter 4, "Administrative Templates for Windows XP."
- **Laptop OU**. This OU contains laptop computers for mobile users that are not always connected to your network. Chapter 3, "Security Settings for Windows XP Clients," and Chapter 4, "Administrative Templates for Windows XP" provide detailed discussion of the settings that are applied to this OU.

# GPO Design to Support Security Management

Use GPOs to ensure that specific policy settings, user rights, and behavior apply to all workstations or users within an OU. The use of Group Policy instead of manual configuration makes it simple to update a number of workstations or users in the future with additional changes. Manual configuration is inefficient, because it requires a technician to visit each client computer. Also, if policy settings in domain–based GPOs are different than those that are applied locally, the domain–based GPO policy settings will overwrite the locally-applied policy settings.

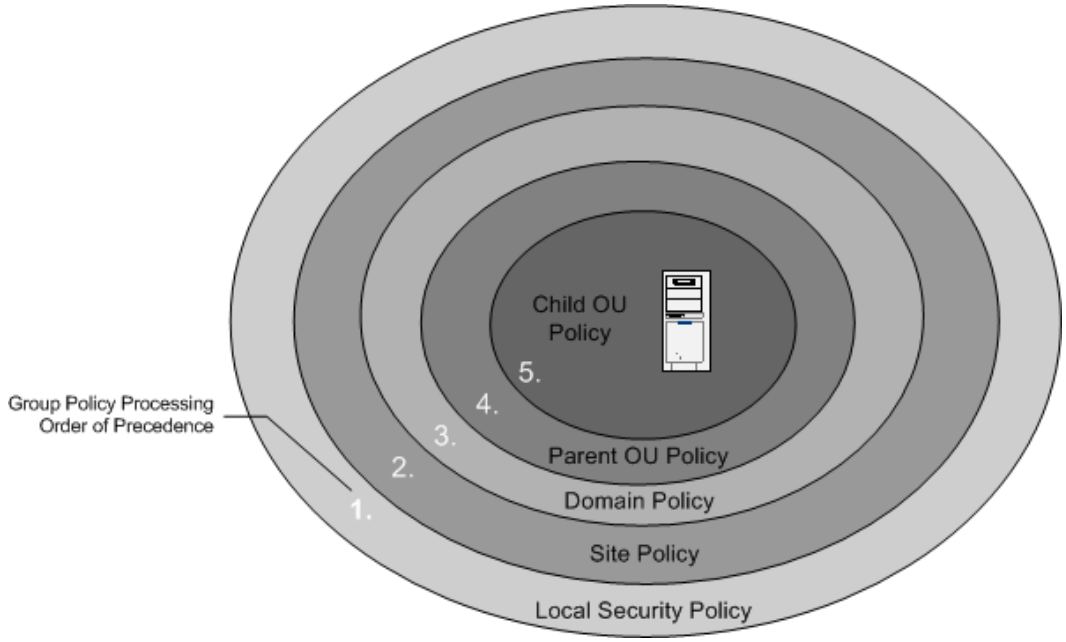


**Figure 2.2 GPO application order**

This figure shows the order in which GPOs are applied to a computer that is a member of the Child OU, from the lowest order (1) to the highest (5). Group Policies are applied first from the local policy of each Windows XP workstation. After the local policies are applied, any GPOs are applied at the site level, and then at the domain level.

For Windows XP client computers that are nested in several OU layers, GPOs are applied in order from the highest OU level in the hierarchy to the lowest. The final GPO is applied from the

OU that contains the client computer. This order of GPO processing—local policy, site, domain, parent OU, and child OU—is significant because GPOs that are applied later in the process will overwrite those applied earlier. User GPOs are applied in the same manner.

The following considerations apply when you design Group Policy.

- An administrator must set the order in which you link multiple GPOs to an OU, or the policies will be applied by default in the order they were linked to the OU. If the same setting is configured in multiple policies, the policy that is highest on the policy list for the container will take precedence.
- You may configure a GPO with the **Enforced** option. If you select this option, other GPOs cannot override the settings that are configured in this GPO.

  **Note**: In Windows 2000, the **Enforced** option is referred to as the **No Override** option.
- You may configure an Active Directory, site, domain, or OU with the **Block policy inheritance** option. This option blocks GPO settings from GPOs that are higher in the Active Directory hierarchy unless they have the **Enforced** option selected. In other words, the **Enforced** option has precedence over the **Block policy inheritance** option.
- Group Policy settings apply to users and computers, and are based on where the user or computer object is located in Active Directory. In some cases, user objects may need policy applied to them based on the location of the computer object, not the location of the user object. The Group Policy loopback feature gives the administrator the ability to apply user Group Policy settings based on which computer the user is logged on to. For more information about loopback support, see the Group Policy white paper that is listed in the “More Information” section at the end of this chapter.

The following figure expands the preliminary OU structure to show how GPOs may be applied to Windows XP client computers that belong to the Laptop and Desktop OUs.

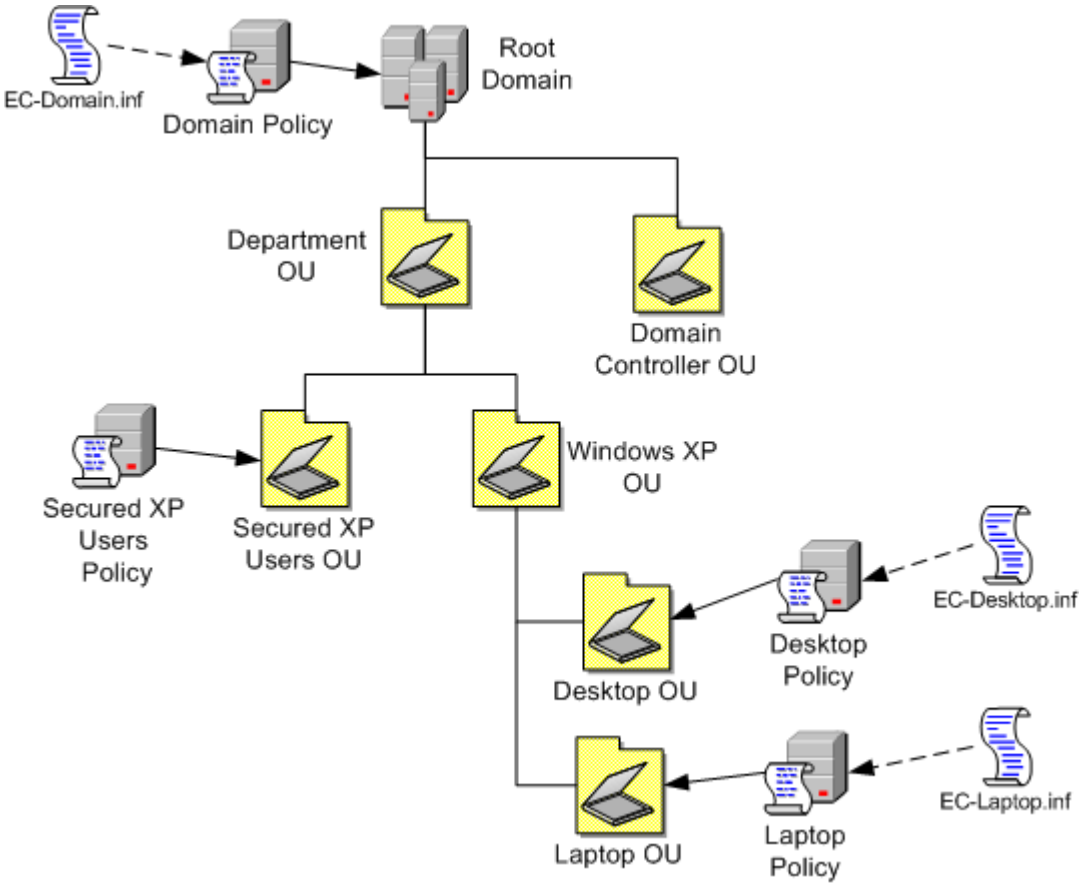


**Figure 2.3 Expanded OU structure to accommodate Windows XP–based desktop and laptop computers**

In the previous example, laptop computers are members of the Laptop OU. The first policy that is applied is the local security policy on the laptop computers. Because there is only one site in this example, no GPO is applied at the site level, which leaves the Domain GPO as the next policy to be applied. Finally, the Laptop GPO is applied.

**Note**: The desktop policy is not applied to any laptops because it is not linked to any OUs in the hierarchy that contains the Laptop OU. Also, the Secured XP Users OU does not have a corresponding security template (.inf file) because it only includes settings from the Administrative Templates.

To show how precedence works, consider an example scenario in which the Windows XP OU policy setting for **Allow logon through Terminal Services** is set to the **Administrators** group and the Laptop GPO setting for **Allow logon through Terminal Services** is set to the **Power Users** and **Administrators** groups. In this example, a user whose account is in the **Power Users** group can log on to a laptop through Terminal Services because the Laptop OU is a child of the Windows XP OU. If the **No Override** policy option in the Windows XP GPO is enabled, only those with accounts in the **Administrators** group are allowed to log on to the client computer through Terminal Services.

# *Security Templates*

Security templates are text files that contain security setting values. They are subcomponents of GPOs, The policy settings that are contained in security templates can be modified in the MMC

Group Policy Object Editor snap-in, and they are located under the **Computer Configuration\Windows Settings\Security Settings** folder. You can also modify these files with the MMC Security Templates snap-in or with a text editor such as Notepad. Microsoft recommends that you use the Group Policy Object Editor snap-in to manage policy settings in security templates that are in GPOs, and that you use the Security Templates snap-in to manage policy settings in stand-alone security templates.

Some sections of the template files contain specific access control lists (ACLs) that are defined by the Security Descriptor Definition Language (SDDL). For details about how to edit security templates and SDDL, see the "More Information" section at the end of this chapter.

## Security Template Management

It is very important to store a production environment's security templates in a secure location in the infrastructure. Access to security templates should only be assigned to the administrators who are responsible for Group Policy implementation. The security templates that are included with Windows XP, Windows 2000, and Windows Server 2003 are stored in the **%SystemRoot%\security\templates** folder by default. As explained in Chapter 1, the security templates that are included with this guide are copied to the **\Windows XP Security Guide Tools and Templates\Security Templates** folder when you execute the .msi file that is included with the WinZip archive file that contains this guide. (The download version of the Windows XP Security Guide is available at http://go.microsoft.com/fwlink/?LinkId=14840.) You may want to copy or move the security templates from this folder to a new location on test computers while you assess and refine the settings to fit your organization's business requirements. After testing is complete, you should move the final versions of the security templates to a centralized location, such as the default location of the built-in security templates.

The **%SystemRoot%\security\templates** folder is not replicated across domain controllers. Therefore, you will need to select a domain controller to hold the master copy of the security templates so that you do not encounter version control problems with the templates. This best practice ensures that you will always modify the same copy of the templates.

## Importing a Security Template

Perform the steps in the following procedure to import a security template.

**To import a security template into a GPO**

1. Navigate to the **Windows Settings** folder in the Group Policy Object Editor.
2. Expand the **Windows Settings** folder and select **Security Settings**.
3. Right-click the **Security Settings** folder, and then click **Import Policy…**
4. Select the security template you want to import, and click **Open**. The settings from the file will be imported into the GPO.

# *Administrative Templates*

Additional security settings are available in Unicode-based files that are called Administrative Templates. These files contain registry settings that affect Windows XP and its components, along with other applications such as Microsoft Office 2003. Administrative Templates may include computer settings as well as user settings. Computer settings are stored in the HKEY_LOCAL_MACHINE registry hive. User settings are stored in the HKEY_CURRENT_USER registry hive.

## Administrative Template Management

It is important to store the Administrative Templates that are used in a production environment in a secure location in the infrastructure, just as it is important to store the security templates securely. Only administrators who are responsible for Group Policy implementation should have access to this location. Administrative Templates that ship with Windows XP and Windows Server 2003 are stored in the **%systemroot%\inf** directory. Additional templates for Office 2003 are included with the *Office 2003 Resource Kit*. The Administrative Templates that are provided by Microsoft should not be edited because they may change when service packs are released.

## Adding an Administrative Template to a Policy

In addition to the Administrative Templates that shipped with Windows XP, you may want to apply the Office 2003 templates to those GPOs in which you want to configure Office 2003 settings. Or you may have created custom Administrative Templates that are unique to your organization. Use the following procedure to add an administrative template to a GPO.

**To add an Administrative Template to a GPO**

1. Navigate to the Administrative Templates folder in the Group Policy Object Editor.
2. Right-click the **Administrative Templates** folder and then click **Add/Remove Templates**.
3. In the **Add/Remove Templates** dialog box, click **Add**.
4. Navigate to the folder containing your Administrative Template files.
5. Select the template you want to add, click **Open**, and then **Close**.

# Domain Level Group Policy

The domain level Group Policy includes settings that apply to all computers and users in the domain. This guide suggests that you configure domain level settings in a new GPO rather than in the built-in Default Domain Policy. The reason for this suggestion is that it will facilitate your ability to restore the default settings if the changes that are introduced in this guide cause problems. You should note that some applications automatically configure the Default Domain Policy, and policy settings that are changed by such applications may conflict with settings that are defined in the Domain Policy GPO that is described in this guide. However, the risk of such an occurrence is small, because only a handful of settings are configured at the domain level. Domain level security is discussed in detail in Chapter 3, “The Domain Policy" of the *Windows Server 2003 Security Guide*, which is available at http://go.microsoft.com/fwlink/?LinkId=14845.

# Password Policy Settings

Complex passwords that change regularly reduce the likelihood of a successful password attack. Password policy settings control the complexity and lifetime of passwords and can only be configured by Group Policy at the domain level. For information about how to set password policies directly in the local Security Account Manager (SAM) on stand-alone computers, see Chapter 5, "Securing Stand-Alone Windows XP Clients."

This section discusses each password policy setting for the EC and SSLF environments.

You can configure the password policy settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**

The following table summarizes the password policy setting recommendations for the two types of secure environments defined in this guide. More detailed information about each of the settings is provided in the following subsections.

**Table 2.1 Password Policy Setting Recommendations**

| Setting | Domain controller default | EC | SSLF |
|---|---|---|---|
| Enforce password history | 24 passwords | 24 passwords | 24 passwords |
| Maximum password age | 42 days | 90 days | 90 days |
| Minimum password age | 1 day | 1 day | 1 day |
| Minimum password length | 7 characters | 8 characters | 12 characters |
| Password must meet complexity requirements | Enabled | Enabled | Enabled |
| Store password using reversible encryption for all users in the domain | Disabled | Disabled | Disabled |

# Enforce password history

This policy setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows XP is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the **Minimum password age** setting to prevent users from repeatedly changing their password.

Configure the **Enforce password history** setting to **24 passwords** for the two security environments that are defined in this guide.

# Maximum password age

Values for this policy setting range from 1 to 999 days. (You may also set the value to 0 to specify that passwords never expire.) This policy setting defines how long a user can use their password before it expires. The default value for this policy setting is 42 days. Most passwords can be cracked; therefore, the more frequently the password is changed the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support.

Configure the **Maximum password age** setting to a value of **90 days** for the two security environments that are defined in this guide.

# Minimum password age

This policy setting determines the number of days that a password must be used before a user may change it. The range of values for this policy setting is between 1 and 998 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this policy setting is 0 days.

The value for the **Minimum password age** setting must be less than that specified for the **Maximum password age** setting, unless the value for the **Maximum password age** setting is configured to 0, which causes passwords never to expire. If the value for the **Maximum password age** setting is configured to 0, the value for this policy setting can be configured to any value between 0 and 999.

If you want the **Enforce password history** setting to be effective, configure this value to be greater than 0. If the **Minimum password age** setting is 0, users can cycle through passwords repeatedly until they can re-use an old favorite.

Configure the **Minimum password age** setting to a value of 1 day for the two security environments that are defined in this guide. This value discourages users from repeated re-use of the same password because it requires them to wait a full day before they can change passwords. It also encourages users to remember new passwords because they must use them for at least a day before they can reset them. Finally, it does not allow users to circumvent the **Enforce password history** setting restriction.

## Minimum password length

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 and later versions, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Remember that users must be educated about the proper selection and maintenance of passwords, especially with regard to password length.

In the EC environment, ensure that the value for the **Minimum password length** setting is configured to **8 characters**. This policy setting is long enough to provide adequate security, but still short enough for users to easily remember. In the SSLF environment, configure the value to **12 characters**.

## Password must meet complexity requirements

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords. By default, the value for this policy setting in Windows XP is configured to **Disabled**, but it is **Enabled** in a Windows Server 2003 domain.

Each additional character in a password increases its complexity exponentially. For instance, a seven-digit all lower-case alphabetic password would have $26^7$ (approximately $8 \times 10^9$ or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has $52^7$ combinations. A seven-character case-sensitive alphanumeric password without punctuation has $62^7$ combinations. An eight-character password has $26^8$ (or $2 \times 10^{11}$) possible combinations. Although this might seem to be a mind-boggling number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as ! or @.

Proper use of the password settings can make it very difficult, if not impossible, to mount a brute force attack.

## Store password using reversible encryption for all users in the domain

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption; it provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords. For this reason, this policy setting should never be enabled unless application requirements outweigh the need to protect password information. The default value for this policy setting is **Disabled**.

This policy setting must be enabled when using the Challenge-Handshake Authentication Protocol (CHAP) through remote access or Internet Authentication Service (IAS). It is also required when using Digest Authentication in Microsoft Internet Information Services (IIS).

Ensure that the **Store password using reversible encryption for all users in the domain** setting is configured to **Disabled**, which is how it is configured in the Default Domain GPO of Windows Server 2003 and in the local security policy for workstations and servers. This policy setting is also **Disabled** in the two environments that are defined in this guide.

## *Preventing Users from Changing Passwords Except When Required*

In addition to the password policies that are described earlier in this chapter, centralized control over all users is a requirement for some organizations. This section describes how to prevent users from changing their passwords except when they are required to do so.

Centralized control of user passwords is a cornerstone of a well-crafted Windows XP security scheme. You can use Group Policy to set minimum and maximum password ages as discussed previously. However, frequent password change requirements can enable users to circumvent the **Enforce password history** setting for your environment. Requirements for passwords that are too long may also lead to more help desk calls from users who forget their passwords.

Users can change their passwords during the period between the minimum and maximum password age settings. However, the Specialized Security – Limited Functionality environment security design requires that users change their passwords only when prompted by the operating system after their passwords have reached the maximum age of 42 days. To achieve this level of control, administrators can disable the **Change Password…** button in the **Windows Security** dialog box that appears when you press CTRL+ALT+DELETE.

You can implement this configuration for an entire domain through Group Policy, or implement it for one or more specific users by editing the registry. For more detailed information about this configuration, see Microsoft Knowledge Base article 324744, "How To: Prevent Users from Changing a Password Except When Required in Windows Server 2003," which is available at http://support.microsoft.com/default.aspx?scid=324744. If you have a Windows 2000 domain, see Microsoft Knowledge Base article 309799, "How To: Prevent Users from Changing a Password Except When Required in Windows 2000" at http://support.microsoft.com/default.aspx?scid=309799.

# Account Lockout Policy Settings

The account lockout policy is an Active Directory security feature that locks a user account and prevents logon after a specified number of failed logon attempts occur within a specified time period. Logon attempts are tracked by domain controllers. The number of allowed attempts and the time period are based on the values that are configured for the account lockout settings. The duration of the lockout can also be specified.

These policy settings help prevent attackers from guessing user passwords, and they decrease the likelihood of successful attacks on your network environment. However, an enabled account lockout policy will probably result in more support issues for network users. Before you enable the following settings, ensure that your organization wants to accept this additional management overhead. For many organizations, an improved and less-costly solution is to automatically scan the Security event logs for domain controllers and generate administrative alerts when it appears that someone is attempting to guess passwords for user accounts.

You can configure the account lockout policy settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy**

The following table includes the account lockout policy setting recommendations for both of the security environments that are defined in this guide. More detailed information about each of the settings is provided in the following subsections.

**Table 2.2 Account Lockout Policy Setting Recommendations**

| Setting | Domain controller default | EC | SSLF |
|---|---|---|---|
| Account lockout duration | Not defined | 15 minutes | 15 minutes |
| Account lockout threshold | 0 invalid logon attempts | 50 invalid logon attempts | 10 invalid logon attempts |
| Reset account lockout counter after | Not defined | 15 minutes | 15 minutes |

# Account lockout duration

This policy setting determines the length of time that must pass before an account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator unlocks them. The Windows XP default value for this policy setting is **Not Defined**.

To reduce the number of help desk support calls and also provide a secure infrastructure, configure the value for the **Account lockout duration** setting to **15** minutes for both the EC and SSLF environments that are defined in this guide.

Although it might seem like a good idea to configure the value for this policy setting to never automatically unlock accounts, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts that were locked by mistake. The recommended setting value of 15 minutes was determined to be a reasonable amount of time for users to wait to log on again if they are locked out of their accounts. Users should also be made aware of how this policy is configured so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer.

# Account lockout threshold

This policy setting determines the number of logon attempts that a user can make before an account is locked. Authorized users can lock themselves out of an account by mistyping their password or by remembering it incorrectly, or by changing their password on one computer while logged on to another computer. The computer with the incorrect password will continuously try to authenticate the user, and because the password it is using to authenticate is incorrect, the user account is eventually locked out. To avoid accidental lockout of authorized users, set the account lockout threshold to a high number. The default value for this policy setting is 0 invalid logon attempts, which disables the account lockout feature.

Configure the value for the **Account lockout threshold** setting to **50** invalid logon attempts for EC environments and **10** for SSLF environments.

Because it is possible for an attacker to use this lockout state as a denial of service (DoS) by triggering a lockout on a large number of accounts, your organization should determine whether

or not to use this policy setting based on identified threats and the risks you wish to mitigate. There are two options to consider for this policy setting.

- Configure the value for **Account lockout threshold** to **0** to ensure that accounts will not be locked out. This setting value will prevent a DoS attack that attempts to lock out accounts in your organization. It will also reduce help desk calls, because users will not be able to lock themselves out of their accounts accidentally. However, this setting value will not prevent a brute force attack. The following defenses should also be considered:
  - A password policy that forces all users to have complex passwords made up of 8 or more characters.
  - A robust auditing mechanism to alert administrators when a series of account lockouts occurs in the environment. For example, the auditing solution should monitor for security event 539, which is a logon failure. This event means that the account was locked out at the time the logon attempt was made.

The second option is:

- Configure the value for **Account lockout threshold** to a value that will provide users with the ability to accidentally mistype their password several times but will lock out the account if a brute force password attack occurs. A setting value of 50 invalid logon attempts for EC environments and 10 for SSLF type environments should ensure adequate security and acceptable usability. This configuration will prevent accidental account lockouts and reduce help desk calls, but will not prevent a DoS attack as described in the previous option.

## *Reset account lockout counter after*

This policy setting determines the length of time before the **Account lockout threshold** resets to zero. The default value for this policy setting is **Not Defined**. If the **Account lockout threshold** is defined, then this reset time must be less than or equal to the value for the **Account lockout duration** setting.

Configure the value for the **Reset account lockout counter after** setting to **15** minutes for both the EC and SSLF environments that are defined in this guide.

If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts as described earlier in this chapter. If no policy is determined to reset the account lockout, administrators would have to manually unlock all accounts. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended setting value of 15 minutes was determined to be a reasonable amount of time that users are likely to accept, which should help to minimize the number of calls that are made to the help desk. Users should also be made aware of how this policy is configured so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer.

# User Rights Assignment Settings

User rights are described in detail in Chapter 3, "Security Settings for Windows XP Clients." However, the **Add workstations to domain** user right should be assigned to all domain controllers and therefore is discussed in this chapter. Additional information about member server and domain controller settings may be found in the Chapters 4 and 5 of the *Windows Server 2003 Security Guide*.

## *Add workstations to domain*

This policy setting allows the user to add a computer to a specific domain.

**Table 2.3 User Rights Assignment Setting Recommendations**

| Setting | Domain controller default | EC | SSLF |
|---|---|---|---|
| Add workstations to domain | Authenticated Users | Administrators | Administrators |

For the **Add workstations to domain** setting to take effect, it must be assigned to the user in a GPO that is applied to all of the domain controllers for the domain. A user who is assigned this right can add up to 10 workstations to the domain. Users who are assigned the **Create Computer Objects** permission for an OU or the Computers container in Active Directory can also join a computer to a domain and add an unlimited number of computers to the domain, regardless of whether they have been assigned the **Add workstations to domain** user right or not.

By default, all users in the **Authenticated Users** group have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.

In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. Some organizations want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage them. Such management efforts can be hampered if users are allowed to add workstations to the domain. Also, this user right provides users with a way to perform activities that are more difficult to trace because they can create additional unauthorized domain computers.

For these reasons, the **Add workstations to domain** user right is assigned only to the **Administrators** group in the two environments that are defined in this guide.

# Security Option Settings

Account policy must be defined in a GPO that is linked at the domain level, such as policy settings in the Default Domain Policy. Domain controllers always obtain account policy from the domain level GPOs, even if there is a different account policy set in a GPO that is applied to the OU that contains the domain controller.

Three security option settings that are similar to account policies should be considered at the domain level. You can configure these security option settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

The following table summarizes the security option setting recommendations for the two types of secure environments that are defined in this guide. More detailed information about each of the settings is provided in the following subsections.

**Table 2.4 Security Option Setting Recommendations**

| Setting | Domain member default | EC | SSLF |
|---|---|---|---|
| Microsoft network server: Disconnect clients when logon hours expire | Not defined | Enabled | Enabled |
| Network Access: Allow anonymous SID/NAME translation | Not defined | Disabled | Disabled |
| Network Security: Force logoff when logon hours expire | Disabled | Enabled | Enabled |

# *Microsoft network server: Disconnect clients when logon hours expire*

This policy setting determines whether to disconnect users who are connected to the local network outside their user account's valid logon hours. This policy setting affects the server message block (SMB) component. When this policy setting is enabled, it causes client computer sessions with the SMB service to be forcibly disconnected when the client's logon hours expire. If it is disabled, an established client computer session is allowed to continue after the client's logon hours have expired. When enabling this policy setting, ensure that the **Network security: Force logoff when logon hours expire** setting is also enabled.

**Note**: Server message block is the foundation for shared resources in Windows networks. Settings that affect SMB will therefore affect shared resources such as folders and printers.

If your organization has configured logon hours for users, then it makes sense to enable the **Microsoft network server: Disconnect clients when logon hours expire** setting. Otherwise, users who are assumed to be unable to access network resources outside of their logon hours may actually be able to access those resources through sessions that were established during allowed hours.

If logon hours are not used in your organization, this policy setting will have no affect, even if it is enabled. If logon hours are used, then user sessions will be terminated when their logon hours expire.

# *Network Access: Allow anonymous SID/NAME translation*

The **Network Access: Allow anonymous SID/NAME translation** setting determines if an anonymous user can request the SID for another user. If this policy setting is enabled on a domain controller, a user who knows an administrator's SID attributes could contact a computer that also has this policy setting enabled and use the SID to obtain the administrator's account information. That person could then use the account to initiate a password guessing attack. The default setting on *member computers* is **Disabled**. However, the default setting for *domain controllers* is **Enabled**. If this policy setting is disabled, the following systems may be unable to communicate with Windows Server 2003–based domains:

- Microsoft Windows NT® 4.0–based Remote Access Service servers.
- Remote Access Service servers that run on Windows 2000–based computers that are located in Windows NT 3.*x* domains or Windows NT 4.0 domains.
- Microsoft SQL Server that run on Windows NT 3.*x*–based or on Windows NT 4.0–based computers.

- SQL Server that runs on Windows 2000–based computers that are located in Windows NT 3.*x* domains or in Windows NT 4.0 domains.
- Users in Windows NT 4.0 resource domain who want to assign permissions to access files, shared folders, and registry objects to user accounts from account domains that contain Windows Server 2003 domain controllers.

### *Network Security: Force logoff when logon hours expire*

The **Network Security: Force logoff when logon hours expire** setting determines whether to disconnect users who are connected to the local network outside their user account's valid logon hours. This policy setting affects the SMB component.

If you enable this policy setting, client computer sessions with the SMB server will be disconnected when the user's logon hours expire and they will be unable to log on to the system until their next allowed access time. If you disable this policy setting, established client computer sessions will be maintained after the user's logon hours expire. To affect domain accounts, this policy setting must be defined in a GPO that is linked to the domain root.

## Kerberos Policy

Policy for the Kerberos version 5 authentication protocol is configured on domain controllers, not member computers of the domain. This policy determines settings that are related to the Kerberos protocol, such as ticket lifetimes and enforcement. Kerberos settings do not exist in the local computer policy. In most environments, the default values for these settings should not be changed. This guidance does not provide any changes for the default Kerberos policy. For more information about these settings, see the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

## OU Level Group Policy

Security settings that are included in the OU Level Group Policy should be specific to the OU. Such settings include both computer settings and user settings. To facilitate manageability and improve security, the section that discusses software restriction policy (SRP) is separated from the other security settings in this guidance. Chapter 6, "Software Restriction Policy for Windows XP Clients," provides detailed information about SRP.

### *Group Policy Security Settings*

You will need to create a GPO for each category of Windows XP computer in your environment. Laptops and desktops are divided into separate OUs in this guidance to apply GPOs that are customized for each of these computer categories.

### *Software Restriction Policy Settings*

Create dedicated GPOs to configure SRP settings in your environment. There are compelling reasons to keep the SRP settings separate from the remaining Group Policy settings. One reason is that SRP is conceptually different from other Group Policy settings. Options are not enabled or disabled, and values are not configured. Instead, SRP requires administrators to identify the set of applications that will be supported, what restrictions will be applied, and how exceptions will be handled. Another reason is to facilitate a quick recovery if a catastrophic mistake is made when

SRP policies are implemented in the production environment: administrators can temporarily disable GPOs where SRP settings are defined and not affect any other security settings.

# Group Policy Tools

Several tools that ship with Windows XP make it easier to work with GPOs. A brief overview of some of these tools is provided in this section. For more information about these tools, see online Help in Windows XP.

## Forcing a Group Policy Update

Active Directory updates Group Policy periodically, but you can force the version on your client computers to be updated with Gpupdate, a command-line tool that ships with Windows XP Professional. The tool must be run locally on client computers.

To update a local computer with this tool, execute the following at a command prompt:

```
gpupdate /force
```

After you run Gpupdate, the following confirmation information will display:

```
C:\Documents and Settings\administrator.MSSLAB>gpupdate /force
Refreshing Policy...
User Policy Refresh has completed.
Computer Policy Refresh has completed.
To check for errors in policy processing, review the event log.
C:\Documents and Settings\administrator.MSSLAB>
```

For user-based Group Policy, you will have to log off and log back on to the computer you are using to test policies. Computer polices should be updated immediately.

To see additional Gpupdate options, execute the following at a command prompt:

```
gpupdate /?
```

## Viewing the Resultant Set of Policies

Two tools that ship with Windows XP allow you to determine what policies have been applied to computers in your environment, when they were applied, and in what order.

- **RSoP Snap-in**. This tool (RSoP.msc) is an MMC snap-in tool that displays the aggregate settings of all policies that have been applied to a computer. The tool may be run locally or remotely from another computer. For each policy setting, the RSoP tool shows the computer setting and the source GPO.
- **Gpresult**. A command-line tool that provides statistics on when Group Policy was most recently applied to a computer, what GPOs were applied to the computer, and in what order. The tool also provides information about any GPOs that were applied through filtering. The Gpresult tool can be used remotely or locally on client computers.

## Group Policy Management Console

The Group Policy Management Console (GPMC) is an MMC snap-in that is available as an optional component with Windows Server 2003 Service Pack 1. It is used to manage all Group Policy-related tasks. GPMC helps to plan, stage, deploy, report, script, and troubleshoot the application of GPOs. More information see the Enterprise Management with the Group Policy

Management Console home page at
http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.

# Summary

Group Policy is an Active Directory–based feature that allows you to control user and computer environments in Windows Server 2003 and Windows 2000 domains. Before you apply Group Policy to the Windows XP desktops in your environment, you must perform certain preliminary steps in your domain.

Group Policy settings that are stored in Group Policy objects (GPOs) on the domain controllers in your environment are linked to sites, domains, and OUs that reside within the Active Directory structure. It is important to understand Active Directory structure and the security implications of configuring different design options within it before you implement Group Policy.

Group Policy is an essential tool for securing Windows XP. This chapter included details about how you can use it to apply and maintain a consistent security policy across your network from a central location.

The chapter also provided information about the different levels of Group Policy and about special tools that can be used to update the Group Policy in your environment.

# More Information

The following links provide additional information about Windows XP Professional security-related topics.

- For more information about Active Directory management and design, see the white paper "Design Considerations for Delegation of Administration in Active Directory" at http://go.microsoft.com/fwlink/?LinkId=18349.
- For more information about Active Directory design, see the white paper "Best Practice Active Directory Design for Managing Windows Networks" at http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/bpaddsgn.mspx.
- For more information about Group Policy, see the white paper "Step-by-Step Guide to Understanding the Group Policy Feature Set" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/gpfeat.mspx.
  Also, see the Windows Server 2003 Group Policy home page at http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.mspx
- For more information about Windows XP Security, see the "Microsoft Windows XP Professional Resource Kit" at http://www.microsoft.com/WindowsXP/pro/techinfo/productdoc/resourcekit.asp.
- For an overview of the security features for Windows XP, see the white paper "What's New in Security for Windows XP Professional and Windows XP Home Edition" at http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/xpsec.mspx.
- For more information about Administrative Templates, see the white paper "Using Administrative Template Files with Registry-Based Group Policy" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx.
- For more information about the Group Policy Management Console (GPMC), see the GPMC site at http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.
- For more information about the Group Policy Update tool (Gpupdate), see http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/refrgp.mspx.
- For more information about the Understanding RSoP (RSoP) tool, see http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/rspoverview.mspx.
- For more information about the Group Policy Results tool (Gpresult), see http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/gpresult.mspx.
- For more information about how to delegate authority in Active Directory, see the *Windows 2000 Resource Kits* section on planning "Distributed Security" at http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/distrib/dsca_pt3_stbp.asp.

# Chapter 3: Security Settings for Windows XP Clients

## Overview

This chapter describes in detail the primary security settings that are configured through Group Policy in a Microsoft® Windows® 2000 or Windows Server™ 2003 Active Directory® directory service domain. Implement the prescribed policy settings to ensure that the desktop and laptop computers in your organization that run Microsoft Windows XP Professional with Service Pack 2 (SP2) are configured securely. Guidance is not provided for all available policy settings in Windows XP, just those that are directly relevant to the security of the computer.

As described in Chapter 1, "Introduction to the Windows XP Security Guide," the guidance that is presented in this chapter is specific to the Enterprise Client (EC) and the Specialized Security – Limited Functionality (SSLF) environments that are defined in this guide. In some instances, this chapter recommends policy settings for laptops that are different than those for desktops because portable computers are mobile and not always connected to domain controllers in your environment through your organization's network. It is also assumed that laptop users sometimes work at different times when on-site technical support is not available. For these reasons, policy settings that require connectivity to a domain controller or that govern logon hours are different for laptop client computers.

Policy settings that are not specified for specific environments are sometimes defined at the domain level, as described in Chapter 2, "Configuring the Active Directory Domain Infrastructure." Other policy settings that are listed as **Not Defined** in this chapter are treated in this manner because the default value is sufficiently secure for that particular environment. Also, undefined policy settings in these Group Policy objects (GPOs) facilitate the deployment of applications that need to modify settings during installation. For example, enterprise management tools may need to assign specific user rights to the local service accounts on managed computers. The guidance in this chapter consists of recommendations, and you should always carefully consider your business needs before you make any changes in your environment.

The following table defines the infrastructure (.inf) files that are available with this guidance. The files contain all of the baseline security setting prescriptions for the two environments that are discussed in this chapter.

**Table 3.1 Baseline Security Templates**

| Description | EC | SSLF |
|---|---|---|
| Baseline security templates for desktops | EC-Desktop.inf | SSLF-Desktop.inf |
| Baseline security templates for laptops | EC-Laptop.inf | SSLF-Laptop.inf |

For more detailed information about the policy settings that are discussed in this chapter, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available for download at http://go.microsoft.com/fwlink/?LinkId=15159.

# Account Policy Settings

Account policy setting information is not provided in this chapter. These settings are discussed in Chapter 2, "Configuring the Active Directory Domain Infrastructure," of this guide.

# Local Policy Settings

Local policy settings may be configured on any computer that runs Windows XP Professional through either the Local Security Policy Console or through the Active Directory domain-based GPOs. Local policy settings include those for Audit policy, user rights assignments, and security options.

# Audit Policy Settings

An Audit policy determines the security events to report to administrators so that user or system activity in specified event categories is recorded. The administrator can monitor security-related activity, such as who accesses an object, when users log on to or log off from computers, or if changes are made to an Audit policy setting. For all of these reasons, Microsoft recommends that you form an Audit policy for an administrator to implement in your environment.

However, before you implement an Audit policy you must decide which event categories need to be audited in your environment. The audit settings you choose within the event categories define your Audit policy. When you define audit settings for specific event categories, an administrator can create an Audit policy that will meet the security needs of your organization.

If no audit settings are configured, it will be difficult or impossible to determine what took place during a security incident. However, if audit settings are configured so that too many authorized activities generate events, the Security event log will fill up with useless data. The information in the following sections is designed to help you decide what to monitor and how to collect relevant audit data for your organization.

You can configure the Audit policy settings in Windows XP at the following location in the Group Policy Object Editor:

> **Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy**

The following table summarizes the Audit policy setting recommendations for both desktop and laptop client computers in the two types of secure environments that are discussed in this chapter. The Enterprise Client environment is referred to as EC, and the Specialized Security – Limited Functionality environment is referred to as SSLF. You should review these recommendations and adjust them as appropriate for your organization. However, be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for **Audit privilege use**, so many audit events will be generated that it may not be feasible to find other types of entries in the Security event log. Such a configuration could also have a significant impact on performance. More detailed information about each of the settings is provided in the following subsections.

**Table 3.2 Audit Policy Setting Recommendations**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Audit account logon events | Success | Success | Success, Failure | Success, Failure |
| Audit account management | Success | Success | Success, Failure | Success, Failure |
| Audit directory service access | Not Defined | Not Defined | Not Defined | Not Defined |
| Audit logon events | Success | Success | Success, Failure | Success, Failure |
| Audit object access | No Auditing | No Auditing | Failure | Failure |
| Audit policy change | Success | Success | Success | Success |
| Audit privilege use | No Auditing | No Auditing | Failure | Failure |
| Audit process tracking | No Auditing | No Auditing | No Auditing | No Auditing |
| Audit system events | Success | Success | Success | Success |

## Audit account logon events

If this policy setting is enabled, events for credential validation are generated. These events occur on the computer that is authoritative for the credentials. For domain accounts the domain controller is authoritative, and for local accounts the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization depending on the accounts that are used to log on.

In this guidance, the **Audit account logon events** setting is configured to **Success** only for the EC environment and to **Success** and **Failure** for the SSLF environment.

## Audit account management

This policy setting is used to track attempts to create new users or groups, rename users or groups, enable or disable user accounts, change account passwords, and enable auditing for Account Management events. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user and group accounts.

The **Audit account management** setting is configured to **Success** for the EC environment and to **Success** and **Failure** for the SSLF environment.

## Audit directory service access

This policy setting can only be enabled to perform audit tasks on domain controllers. For this reason, the setting is not defined at the workstation level. This policy setting does not apply to computers that run Windows XP Professional. Therefore, ensure that the **Audit directory service access** setting is configured to **Not Defined** for the two environments that are discussed in this chapter.

## Audit logon events

This policy setting generates events that record the creation and destruction of logon sessions. These events occur on the computer that is accessed. For interactive logons, these events would

be generated on the computer that was logged on to. If a network logon was performed to access a share, these events would be generated on the computer that hosts the resource that was accessed.

If you configure the **Audit logon events** setting to **No auditing**, it is difficult or impossible to determine which user has either accessed or attempted to access computers in the organization.

The **Audit logon events** setting is configured to log **Success** events for the EC environment. This policy setting is configured to **Success** and **Failure** events for the SSLF environment.

# *Audit object access*

By itself, this policy setting will not cause any events to be audited. It determines whether to audit the event of a user who accesses an object—for example, a file, folder, registry key, or printer—that has a specified system access control list (SACL).

A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:

- The security principal (user, computer, or group) to be audited.
- The specific access type to be audited, called an access mask.
- A flag to indicate whether to audit failed access events, successful access events, or both.

If you configure the **Audit object access** setting to **Success**, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to **Failure**, an audit entry is generated each time that a user unsuccessfully attempts to access an object with a specified SACL.

Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the **Write and Append Data auditing** setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed.

The **Audit object access** setting is configured to **No Auditing** for the EC environment and to **Failure** for the SSLF environment. You must enable this setting for the following procedures to take effect.

The following procedures detail how to manually set up audit rules on a file or folder and how to test each audit rule for each object in the specified file or folder. The testing procedure may be automated by means of a script file.

**To define an audit rule for a file or folder**

1. Locate the file or folder using Windows Explorer and select it.
2. Click the **File** menu and select **Properties**.
3. Click the **Security** tab, and then click the **Advanced** button.
4. Click the **Auditing** tab.
5. Click the **Add** button, and the **Select User, Computer, or Group** dialog box will display.
6. Click the **Object Types…** button, and in the **Object Types** dialog box select the object types you want to find.

   **Note**: The User, Group, and Built-in security principal object types are selected by default.
7. Click the **Locations…** button, and in the **Location:** dialog box select either your domain or local computer.
8. In the **Select User or Group** dialog box, type the name of the group or user you want to audit. Then, in the **Enter the object names to select** dialog box, type **Authenticated Users**

(to audit the access of all authenticated users) and click **OK**. The **Auditing Entry** dialog box will display.

9. Determine the type of access you want to audit on the file or folder using the **Auditing Entry** dialog box.

   **Note**: Remember that each access may generate multiple events in the event log and cause it to grow rapidly.

10. In the **Auditing Entry** dialog box, next to **List Folder** / **Read Data**, select **Successful and Failed**, and then click **OK**.
11. The audit entries you have enabled will display under the **Auditing** tab of the **Advanced Security Setting** dialog box.
12. Click **OK** to close the **Properties** dialog box.

**To test an audit rule for the file or folder**

1. Open the file or folder.
2. Close the file or folder.
3. Start the Event Viewer. Several Object Access events with **Event ID 560** will appear in the Security event log.
4. Double-click the events as needed to view their details.

# Audit policy change

This policy setting determines whether to audit every incident of a change to user rights assignment policies, Windows Firewall policies, Trust policies, or changes to the Audit policy itself. The recommended settings would let you see any account privileges that an attacker attempts to elevate—for example, by adding the **Debug programs** privilege or the **Back up files and directories** privilege.

The **Audit policy change** setting is configured to **Success** for the two environments that are discussed in this chapter. The setting value for **Failure** is not included because it will not provide meaningful access information in the Security event log.

# Audit privilege use

This policy setting determines whether to audit each instance of a user exercising a user right. If you configure this value to **Success**, an audit entry is generated each time that a user right is exercised successfully. If you configure this value to **Failure**, an audit entry is generated each time that a user right is exercised unsuccessfully. This policy setting can generate a very large number of event records.

The **Audit privilege use** setting is configured to **No Auditing** for computers in the EC environment and to **Failure** for the SSLF environment to audit all unsuccessful attempts to use privileges.

# Audit process tracking

This policy setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Enabling **Audit process tracking** will generate a large number of events, so typically it is set to **No Auditing**. However, this setting can provide a great benefit during an incident response from the detailed log of the processes started and the time when they were launched.

The **Audit process tracking** setting is configured to **No Auditing** for the two environments that are discussed in this chapter.

## *Audit system events*

This policy setting is very important because it allows you to monitor system events that succeed and fail, and provides a record of these events that may help determine instances of unauthorized system access. System events include starting or shutting down computers in your environment, full event logs, or other security-related events that affect the entire system.

The **Audit system events** setting is configured to **Success** for both of the environments that are discussed in this chapter.

# User Rights Assignment Settings

In conjunction with many of the privileged groups in Windows XP Professional, a number of user rights may be assigned to certain users or groups that typical users do not have.

To set the value of a user right to **No One**, enable the setting but do not add any users or groups to it. To set the value of a user right to **Not Defined**, do not enable the setting.

You can configure the user rights assignment settings in Windows XP at the following location in the Group Policy Object Editor:

> **Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment**

The following table summarizes user rights assignment setting recommendations for user rights that begin with the letters A through E. Recommendations are provided for both desktop and laptop client computers in the two types of secure environments that are discussed in this chapter. More detailed information about each of the settings is provided in the following subsections.

Recommendations for user rights that begin with the rest of the letters in the alphabet are summarized in Table 3.4, and additional detailed information about those user rights is provided in the subsections that follow that table.

**Note**: Many features in Internet Information Server (IIS) require certain accounts such as IIS_WPG, IIS IUSR_<*ComputerName*>, and IWAM_<*ComputerName*> to have specific privileges. For more information about what user rights are required by accounts that are related to IIS, see "IIS and Built-in Accounts (IIS 6.0)" at http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/3648346f-e4f5-474b-86c7-5a86e85fa1ff.mspx.

# User Rights A – E

**Table 3.3 User Rights Assignment Setting Recommendations – Part 1**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Access this computer from network | Not Defined | Not Defined | Administrators | Administrators |
| Act as part of the operating system | No One | No One | No One | No One |
| Adjust memory quotas for a process | Not Defined | Not Defined | Administrators, Local Service, Network Service | Administrators, Local Service, Network Service |
| Allow log on locally | Users, Administrators | Users, Administrators | Users, Administrators | Users, Administrators |
| Allow log on through Terminal Services | Not Defined | Not Defined | No One | No One |
| Back up files and directories | Not Defined | Not Defined | Administrators | Administrators |
| Bypass traverse checking | Not Defined | Not Defined | Administrators, Users | Administrators, Users |
| Change the system time | Administrators | Administrators | Administrators | Administrators |
| Create a pagefile | Administrators | Administrators | Administrators | Administrators |
| Create permanent shared objects | Not Defined | Not Defined | No One | No One |
| Create a token object | Not Defined | Not Defined | No One | No One |
| Debug programs | Administrators | Administrators | No One | No One |
| Deny access to this computer from the network | Support_ 388945a0, Guest | Support_ 388945a0, Guest | Support_ 388945a0, Guest | Support_ 388945a0, Guest |
| Deny log on as a batch job | Not Defined | Not Defined | Support_ 388945a0, Guest | Support_ 388945a0, Guest |
| Deny log on locally | Not Defined | Not Defined | Support_ 388945a0, Guest, any service accounts | Support_ 388945a0, Guest, any service accounts |
| Deny log on through Terminal Services | Not Defined | Not Defined | Everyone | Everyone |
| Enable computer and user accounts to be trusted for delegation | Not Defined | Not Defined | No One | No One |

## Access this computer from network

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)–based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

The **Access this computer from network** setting is configured to **Not Defined** for the EC environment and to **Administrators** for the SSLF environment.

## Act as part of the operating system

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access.

For this reason, the **Act as part of the operating system** setting is restricted to **No One** for both of the environments that are discussed in this chapter.

## Adjust memory quotas for a process

This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack.

For this reason, the **Adjust memory quotas for a process** setting is restricted to **Administrators**, **Local Service**, and **Network Service** for both computer types for the SSLF environment and configured to **Not Defined** for computers for the EC environment.

## Allow log on locally

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or Microsoft Internet Information Services (IIS) also require this user right.

The **Guest** account is assigned this user right by default. Although this account is disabled by default, Microsoft recommends that you enable this setting through Group Policy. However, this user right should generally be restricted to the **Administrators** and **Users** groups. Assign this user right to the **Backup Operators** group if your organization requires that they have this capability.

The **Allow log on locally** setting is restricted to the **Users** and **Administrators** groups for the two environments that are discussed in this chapter.

## Allow log on through Terminal Services

This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, then assign this user right only to the **Administrators** group or use the restricted groups feature to ensure that no user accounts are part of the **Remote Desktop Users** group.

Restrict this user right to the **Administrators** group, and possibly the **Remote Desktop Users** group, to prevent unwanted users from gaining access to computers on your network by means of the new Remote Assistance feature in Windows XP Professional.

The **Allow log on through Terminal Services** setting is configured to **Not Defined** for the EC environment. For additional security this policy setting is configured to **No One** for the SSLF environment.

## Backup files and directories

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply.

The **Back up files and directories** setting is configured to **Not Defined** for computers in the EC environment. This policy setting is configured to the **Administrators** group for the SSLF environment.

## Bypass traverse checking

This policy setting allows users who do not have the special “Traverse Folder” access permission to “pass through” folders when they navigate an object path in the NTFS file system or in the registry. This user right does not allow users to list the contents of a folder, but only allows them to traverse directories.

The **Bypass traverse checking** setting is configured to **Not Defined** for computers in the EC environment. It is configured to the **Administrators** and **Users** groups for the SSLF environment.

## Change the system time

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer’s time setting is changed, logged events reflect the new time, not the actual time that the events occurred.

The **Change the system time** setting is configured to the **Administrators** group for both of the environments that are discussed in this chapter.

**Note**: Discrepancies between the time on the local computer and on the domain controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the domain controllers.

## Create a pagefile

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer.

The **Create a pagefile** setting is configured to the **Administrators** for all computers for both the EC environment and the SSLF environment.

## Create permanent shared objects

This policy setting allows users to create directory objects in the object manager. This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right.

The **Create permanent shared objects** setting is configured to **Not Defined** for the EC environment and to **No One** for the SSLF environment.

## Create a token object

This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data. In environments where security is a high priority, this user right should not be assigned to any users. Any processes that require this capability should use the Local System account, which is assigned this user right by default.

The **Create a token object** setting is configured to **Not Defined** for the EC environment and to **No One** for the SSLF environment.

## Debug programs

This policy setting determines which users can attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. This user right is required when administrators want to take advantage of patches that support "in-memory patching," also known as "hotpatching." For more information about the latest features in the Microsoft Package Installer, see "The Package Installer (Formerly Called Update.exe) for Microsoft Windows Operating Systems and Windows Components" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/deployment/winupdte.mspx. Because an attacker could exploit this user right, it is assigned only to the **Administrators** group by default.

**Note**: Microsoft released several security patches in October 2003 that used a version of Update.exe that required the administrator to have the **Debug programs** user right. Administrators who did not have this user right were unable to install these patches until they reconfigured their user rights. For more information, see the Microsoft Knowledge Base article "Windows Product Updates may stop responding or may use most or all the CPU resources" at http://support.microsoft.com/default.aspx?kbid=830846.

The **Debug programs** user right is very powerful. Therefore, this policy setting is configured to **Administrators** for the EC environment and maintained at its default setting of **No One** for the SSLF environment.

## Deny access to this computer from the network

This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In a high security environment, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers.

The **Deny access to this computer from the network** setting is configured to the **Support_388945a0** and **Guest** accounts for computers in both of the environments that are discussed in this chapter.

## Deny log on as a batch job

This policy setting prohibits user logon through a batch-queue facility, a feature in Windows Server 2003 that is used to schedule jobs to run automatically one or more times in the future.

The **Deny log on as a batch job** setting is configured to **Not Defined** for the EC environment and to **Support_388945a0** and **Guest** for the SSLF environment.

## Deny log on locally

This policy setting prohibits users from local logon to the computer console. If unauthorized users could log on locally to a computer, they could download malicious code or elevate their privileges on the computer. (If attackers have physical access to the console, there are other risks to consider.) This user right should not be assigned to those users who need physical access to the computer console.

The **Deny log on locally** setting is configured to **Not Defined** for the EC environment and to **Support_388945a0** and **Guest** for the SSLF environment. Also, any service accounts for the SSLF environment that are added to the computer should be assigned this user right to prevent their abuse.

## Deny log on through Terminal Services

This policy setting prohibits users from logging on to computers in your environment through Remote Desktop connections. If you assign this user right to the **Everyone** group, you also prevent members of the default **Administrators** group from using Terminal Services to log on to computers in your environment.

The **Deny log on through Terminal Services** setting is configured to **Not Defined** for the EC environment and to the **Everyone** group for the SSLF environment.

## Enable computer and user accounts to be trusted for delegation

This policy setting allows users to change the **Trusted for Delegation** setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.

For this reason, the **Enable computer and user accounts to be trusted for delegation** setting is configured to **Not Defined** for the EC environment and to **No One** for the SSLF environment.

# User Rights F –T

**Table 3.4 User Rights Assignment Setting Recommendations – Part 2**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Force shutdown from a remote system | Administrators | Administrators | Administrators | Administrators |
| Generate Security Audits | Local Service, Network Service | Local Service, Network Service | Local Service, Network Service | Local Service, Network Service |
| Increase scheduling priority | Administrators | Administrators | Administrators | Administrators |
| Load and unload device drivers | Administrators | Administrators | Administrators | Administrators |
| Lock pages in memory | No One | No One | No One | No One |
| Log on as a batch job | Not Defined | Not Defined | No One | No One |
| Log on as a service | Not Defined | Not Defined | Network Service, Local Service | Network Service, Local Service |
| Manage auditing and security log | Administrators | Administrators | Administrators | Administrators |
| Modify firmware environment variables | Administrators | Administrators | Administrators | Administrators |
| Perform volume maintenance tasks | Administrators | Administrators | Administrators | Administrators |
| Profile single process | Not Defined | Not Defined | Administrators | Administrators |
| Profile system performance | Administrators | Administrators | Administrators | Administrators |
| Remove computer from docking station | Administrators, Users | Administrators, Users | Administrators, Users | Administrators, Users |
| Replace a process level token | Local Service, Network Service | Local Service, Network Service | Local Service, Network Service | Local Service, Network Service |
| Restore files and directories | Not Defined | Not Defined | Administrators | Administrators |
| Shut down the system | Administrators, Users | Administrators, Users | Administrators, Users | Administrators, Users |
| Take ownership of files or other objects | Administrators | Administrators | Administrators | Administrators |

This table summarizes user rights assignment setting recommendations for user rights that begin with the letters F through T. More detailed information about each of the settings is provided in the following subsections.

## Force shutdown from a remote system

This policy setting allows users to shut down Windows XP–based computers from remote locations on the network. Anyone that has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, Microsoft recommends that only highly trusted administrators be assigned this user right.

The **Force shutdown from a remote system** setting is configured to the **Administrators** group for both of the environments that are discussed in this chapter.

## Generate Security Audits

This policy setting determines which users or processes can generate audit records in the Security log. An attacker could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by a large number of unrelated events.

For this reason, the **Generate Security Audits** setting is configured to the **Local Service** and **Network Service** groups for both of the environments that are discussed in this chapter.

## Increase scheduling priority

This policy setting allows users to change the amount of processor time that a process utilizes. An attacker could use this capability to increase the priority of a process to real-time and create a denial of service condition for a computer.

For this reason, the **Increase scheduling priority** setting is configured to the **Administrators** group for both of the environments that are discussed in this chapter.

## Load and unload device drivers

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right and membership in either the **Power Users** group or the **Administrators** group is required for users to add local printers or printer drivers in Windows XP.

Because this user right could be used by an attacker, the **Load and unload device drivers** setting is configured to the **Administrators** group for both of the environments that are discussed in this chapter.

## Lock pages in memory

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur.

For this reason, the **Lock pages in memory** setting is configured to **No One** for both of the environments that are discussed in this chapter.

## Log on as a batch job

This policy setting allows accounts to log on using the task scheduler service. Because the task scheduler is often used for administrative purposes, it may be needed in the EC environment. However, its use should be restricted in the SSLF environment to prevent misuse of system resources or to prevent attackers from using the right to launch malicious code after gaining user level access to a computer.

Therefore, the **Log on as a batch job** user right is configured to **Not Defined** for the EC environment and to **No One** for the SSLF environment.

## Log on as a service

This policy setting allows accounts to launch network services or to register a process as a service running on the system. This user right should be restricted on any computer in a SSLF environment, but because many applications may require this privilege, it should be carefully evaluated and tested before configuring it in an EC environment.

The **Log on as a service** setting is configured to **Not Defined** for the EC environment and to **Network Service** and **Local Service** for the SSLF environment.

## Manage auditing and security log

This policy setting determines which users can change the auditing options for files and directories as well as clear the Security log.

Because this capability represents a relatively small threat, the **Manage auditing and security log** setting enforces the default value of the **Administrators** group for both of the environments that are discussed in this chapter.

## Modify firmware environment variables

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values and could lead to a hardware failure that would result in a denial of service condition.

Because this capability represents a relatively small threat, the **Modify firmware environment variables** setting enforces the default value of the **Administrators** group for both of the environments that are discussed in this chapter.

## Perform volume maintenance tasks

This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial of service condition.

The **Perform volume maintenance tasks** setting enforces the default value of the **Administrators** group for both of the environments that are discussed in this chapter.

## Profile single process

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the **Profile single process** user right prevents intruders from gaining additional information that could be used to mount an attack on the system.

The **Profile single process** setting is configured to **Not defined** for computers in the EC environment and to the **Administrators** group for the SSLF environment.

## Profile system performance

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer.

The **Profile system performance** setting enforces the default of the **Administrators** group for both of the environments that are discussed in this chapter.

## Remove computer from docking station

This policy setting allows the user of a portable computer to click **Eject PC** on the **Start** menu to undock the computer.

The **Remove computer from docking station** setting is configured to the **Administrators** and **Users** groups for both of the environments that are discussed in this chapter.

## Replace a process level token

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges.

The **Replace a process level token** setting is configured to the default values of **Local Service** and **Network Service** for both of the environments that are discussed in this chapter.

## Restore files and directories

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows XP in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the **Back up files and directories** user right.

The **Restore files and directories** setting is configured to **Not Defined** for the EC environment and to the **Administrators** group for the SSLF environment.

## Shut down the system

This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. In high security environments, Microsoft recommends that this right only be assigned to the **Administrators** and **Users** groups.

The **Shut down the system** setting is configured to the **Administrators** and **Users** groups for both of the environments that are discussed in this chapter.

## Take ownership of files or other objects

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects and give ownership to the specified user.

The **Take ownership of files or other objects** setting is configured to the default value of the **Administrators** group for both of the environments that are discussed in this chapter.

# Security Option Settings

The security option settings that are applied through Group Policy on computers that run Windows XP in your environment are used to enable or disable capabilities and features such as floppy disk drive access, CD-ROM drive access, and logon prompts. These settings are also used to configure various other settings, such as those for the digital signing of data, administrator and guest account names, and how driver installation works.

You can configure the security option settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

Not all of the settings that are included in this section exist on all types of systems. Therefore, the settings that comprise the Security Options portion of Group Policy that are defined in this section may need to be manually modified on systems in which these settings are present to make them fully operable. Alternatively, the Group Policy templates can be edited individually to include the appropriate setting options so that the prescribed settings will take full effect.

The following sections provide security option setting recommendations, and are grouped by type of object. Each section includes a table that summarizes the settings, and detailed information is provided in the subsections that follow each table. Recommendations are provided for both desktop and laptop client computers in the two types of secure environments that are discussed in this chapter—the Enterprise Client (EC) environment and the Specialized Security – Limited Functionality (SSLF) environment.

# *Accounts*

The following table summarizes the recommended security option settings for accounts. Additional information is provided in the subsections that follow the table.

**Table 3.5 Security Option Setting Recommendations – Accounts**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Accounts: Administrator account status | Not Defined | Not Defined | Enabled | Enabled |
| Accounts: Guest account status | Disabled | Disabled | Disabled | Disabled |
| Accounts: Limit local account use of blank passwords to console logon only | Enabled | Enabled | Enabled | Enabled |
| Accounts: Rename administrator account | Recommended | Recommended | Recommended | Recommended |
| Accounts: Rename guest account | Recommended | Recommended | Recommended | Recommended |

## Accounts: Administrator account status

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured.

The **Accounts: Administrator account status** setting is configured to **Not Defined** for the EC environment and to **Enabled** for the SSLF environment.

## Accounts: Guest account status

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system.

The **Accounts: Guest account status** security option setting is configured to **Disabled** for the two environments that are discussed in this chapter.

## Accounts: Limit local account use of blank passwords to console logon only

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts with blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer.

The **Accounts: Limit local account use of blank passwords to console logon only** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Accounts: Rename administrator account

The built-in local administrator account is a well-known account name that attackers will target. Microsoft recommends that you choose another name for this account, and that you avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console).

The recommendation to use the **Accounts: Rename administrator account** setting applies to both of the environments that are discussed in this chapter.

**Note**: This policy setting is not configured in the security templates, nor is a new username for the account suggested in this guidance. Suggested usernames are omitted to ensure that organizations that implement this guidance will not use the same new username in their environments.

## Accounts: Rename guest account

The built-in local guest account is another well-known name to hackers. Microsoft also recommends that you rename this account to something that does not indicate its purpose. Even if you disable this account (which is recommended), ensure that you rename it for added security.

The recommendation to use the **Accounts: Rename guest account** setting applies to both of the environments that are discussed in this chapter.

**Note**: This policy setting is not configured in the security templates, nor is a new username for the account suggested here. Suggested usernames are omitted to ensure that organizations that implement this guidance will not use the same new username in their environments.

# *Audit*

The following table summarizes the recommended Audit settings. Additional information is provided in the subsections that follow the table.

**Table 3.6 Security Option Setting Recommendations – Audit**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Audit: Audit the access of global system objects | Not Defined | Not Defined | Disabled | Disabled |
| Audit: Audit the use of Backup and Restore privilege | Not Defined | Not Defined | Disabled | Disabled |
| Audit: Shut down system immediately if unable to log security audits | Not Defined | Not Defined | Not Defined | Not Defined |

## Audit: Audit the access of global system objects

This policy setting creates a default System Access Control List (SACL) for system objects such as mutexes, events, semaphores, and MS-DOS® devices, and causes access to these system objects to be audited.

If the **Audit: Audit the access of global system objects** setting is enabled, a very large number of security events could quickly fill the Security event log. Therefore, this policy setting is configured to **Not Defined** for the EC environment and **Disabled** for the SSLF environment.

## Audit: Audit the use of Backup and Restore privilege

This policy setting determines whether to audit the use of all user privileges, including Backup and Restore, when the **Audit privilege use** setting is in effect. If you enable both policies, an audit event will be generated for every file that is backed up or restored.

If the **Audit: Audit the use of Backup and Restore privilege** setting is enabled, a very large number of security events could quickly fill the Security event log. Therefore, this policy setting is configured to **Not Defined** for the EC environment and **Disabled** for the SSLF environment.

## Audit: Shut down system immediately if unable to log security audits

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason.

If the **Audit: Shut down system immediately if unable to log security audits** setting is enabled, unplanned system failures can occur. Therefore, this policy setting is configured to **Not Defined** for both of the environments that are discussed in this chapter.

# *Devices*

The following table summarizes the recommended security option settings for devices. Additional information is provided in the subsections that follow the table.

**Table 3.7 Security Option Setting Recommendations – Devices**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Devices: Allow undock without having to log on | Not Defined | Not Defined | Disabled | Disabled |
| Devices: Allowed to format and eject removable media | Administrator, Interactive Users | Administrator, Interactive Users | Administrators | Administrators |
| Devices: Prevent users from installing printer drivers | Enabled | Disabled | Enabled | Disabled |
| Devices: Restrict CD-ROM access to locally logged on user only | Not Defined | Not Defined | Disabled | Disabled |

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Devices: Restrict floppy access to locally logged on user only | Not Defined | Not Defined | Disabled | Disabled |
| Devices: Unsigned driver installation behavior | Warn but allow installation | Warn but allow installation | Warn but allow installation | Warn but allow installation |

## Devices: Allow undock without having to log on

This policy setting determines whether a portable computer can be undocked if the user does not log on to the system. Enable this policy setting to eliminate a logon requirement and allow use of an external hardware eject button to undock the computer. If you disable this policy setting, a user who is not logged on must have been assigned the **Remove computer from docking station** user right (not defined in this guidance).

The **Devices: Allow undock without having to log on** setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Devices: Allowed to format and eject removable media

This policy setting determines who is allowed to format and eject removable media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges.

The **Devices: Allow to format and eject removable media** setting is restricted to the **Administrators** and **Interactive Users** groups for the EC environment, and to the **Administrators** group only for the SSLF environment for added security.

## Devices: Prevent users from installing printer drivers

It is feasible for a hacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network. To reduce the possibility of such an event, only administrators should be allowed to install printer drivers. However, because laptops are mobile devices, laptop users may need to occasionally install a printer driver from a remote source in order to continue their work. Therefore, this policy setting should be disabled for laptop users, but always enabled for desktop users.

The **Devices: Prevent users from installing printer drivers** setting is configured to **Enabled** for desktops in both of the environments that are discussed in this chapter and to **Disabled** for laptop users in both of the environments.

## Devices: Restrict CD-ROM access to locally logged on user only

This policy setting determines whether the CD-ROM drive is accessible to both local and remote users simultaneously. If you enable this policy setting, only interactively logged on users are allowed to access media from the CD-ROM drive. When this policy setting is enabled and no one is logged on, the CD-ROM drive can be accessed over the network. If you enable this setting, the Windows Backup utility will fail if volume shadow copies were specified for the backup job. Any third-party backup products that use volume shadow copies will also fail.

The **Devices: Restrict CD-ROM access to locally logged on user only** setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Devices: Restrict floppy access to locally logged on user only

This policy setting determines whether the floppy drive is accessible to both local and remote users simultaneously. If you enable this policy setting, only interactively logged on users are allowed to access floppy drive media. When this policy setting is enabled and no one is logged on, floppy drive media can be accessed over the network. If you enable this setting, the Windows Backup utility will fail if volume shadow copies were specified for the backup job. Any third-party backup products that use volume shadow copies will also fail.

The **Devices: Restrict floppy access to locally logged on user only** setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Devices: Unsigned driver installation behavior

This policy setting determines what happens when an attempt is made to install a device driver (by means of the Setup API) that has not been approved and signed by the Windows Hardware Quality Lab (WHQL). This option prevents the installation of unsigned drivers or warns the administrator that an unsigned driver is about to be installed, which can prevent installation of drivers that have not been certified to run on Windows XP. If you configure this policy setting to the **Warn but allow installation** value, one potential problem is that unattended installation scripts will fail when they attempt to install unsigned drivers.

For this reason, the **Devices: Unsigned driver installation behavior** setting is configured to the **Warn but allow installation** for both of the environments that are discussed in this chapter.

**Note**: If you implement this policy setting, the client computers should be fully configured with all of your standard software applications before Group Policy is applied to mitigate the risk of installation errors that are caused by the setting.

# *Domain Member*

The following table summarizes the recommended security option settings for domain members. Additional information is provided in the subsections that follow the table.

**Table 3.8 Security Option Setting Recommendations – Domain Member**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Domain member: Digitally encrypt or sign secure channel data (always) | Enabled | Enabled | Enabled | Enabled |
| Domain member: Digitally encrypt secure channel data (when possible) | Enabled | Enabled | Enabled | Enabled |
| Domain member: Digitally sign secure channel data (when possible) | Enabled | Enabled | Enabled | Enabled |
| Domain member: Disable machine account password changes | Disabled | Disabled | Disabled | Disabled |
| Domain member: Maximum machine account password age | 30 days | 30 days | 30 days | 30 days |
| Domain member: Require strong (Windows 2000 or later) session key | Enabled | Enabled | Enabled | Enabled |

## Domain member: Digitally encrypt or sign secure channel data (always)

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. If a system is set to always encrypt or sign secure channel data, then it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data is signed and encrypted.

The **Domain member: Digitally encrypt or sign secure channel data (always)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

## Domain member: Digitally encrypt secure channel data (when possible)

This policy setting determines whether a domain member may attempt to negotiate encryption for all secure channel traffic that it initiates. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will be prevented from negotiating secure channel encryption.

The **Domain member: Digitally encrypt secure channel data (when possible)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

## Domain member: Digitally sign secure channel data (when possible)

This policy setting determines whether a domain member may attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.

The **Domain member: Digitally sign secure channel data (when possible)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

## Domain member: Disable machine account password changes

This policy setting determines whether a domain member may periodically change its computer account password. If you enable this policy setting, the domain member will be prevented from changing its computer account password. If you disable this policy setting, the domain member can change its computer account password as specified by the **Domain Member: Maximum machine account password age** setting, which by default is every 30 days. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker may be able to determine the password for the system's domain account.

Therefore, the **Domain member: Disable machine account password changes** setting is configured to **Disabled** for both of the environments that are discussed in this chapter.

## Domain member: Maximum machine account password age

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly or set it to 0 so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts.

Therefore, the **Domain member: Maximum machine account password age** setting is configured to **30 days** for both of the environments that are discussed in this chapter.

## Domain member: Require strong (Windows 2000 or later) session key

When this policy setting is enabled, a secure channel may only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.

To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. If communication to non-Windows 2000 domains is required, Microsoft recommends that you disable this policy setting.

The **Domain member: Require strong (Windows 2000 or later)** session key setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

# *Interactive Logon*

The following table summarizes the recommended security option settings for interactive logon. Additional information is provided in the subsections that follow the table.

**Table 3.9 Security Option Setting Recommendations – Interactive Logon**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Interactive Logon: Do not display last user name | Enabled | Enabled | Enabled | Enabled |
| Interactive Logon: Do not require CTRL+ALT+DEL | Disabled | Disabled | Disabled | Disabled |
| Interactive Logon: Message text for users attempting to log on | This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. | This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. | This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. | This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. |
| Interactive Logon: Message title for users attempting to log on | IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZA-TION. | IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZA-TION. | IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZA-TION. | IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZA-TION. |
| Interactive Logon: Number of previous logons to cache (in case domain controller is not available) | 2 | 2 | 0 | 2 |
| Interactive Logon: Prompt user to change password before expiration | 14 days | 14 days | 14 days | 14 days |

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Interactive Logon: Require Domain Controller authentication to unlock workstation | Enabled | Disabled | Enabled | Disabled |
| Interactive Logon: Smart card removal behavior | Lock Workstation | Lock Workstation | Lock Workstation | Lock Workstation |

## Interactive Logon: Do not display last user name

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization.

The **Interactive logon: Do not display last user name** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Interactive Logon: Do not require CTRL+ALT+DEL

The CTRL+ALT+DEL key combination establishes a trusted path to the operating system when a user enters a username and password. When this policy setting is enabled, users are not required to use this key combination to log on to the network. However, this configuration poses a security risk because it provides an opportunity for users to log on with weaker logon credentials.

The **Interactive logon: Do not require CTRL+ALT+DEL** setting is configured to **Disabled** for the two environments that are discussed in this chapter.

## Interactive Logon: Message text for users attempting to log on

This policy setting specifies a text message that displays to users when they log on. This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. The message text that is specified in the previous table is a recommended example for both the EC and SSLF environments.

The **Interactive Logon: Message text for users attempting to log on** setting is enabled with suitable text for both of the environments that are discussed in this chapter.

**Note**: Any warning that you display should first be approved by your organization's legal and human resources representatives. Also, the **Interactive logon: Message text for users attempting to log on** and the **Interactive logon: Message title for users attempting to log on** settings must both be enabled for either one to work properly.

## Interactive Logon: Message title for users attempting to log on

This policy setting allows text to be specified in the title bar of the window that users see when they log on to the system. The reason for this policy setting is the same as for the previous message text setting. Organizations that do not use this policy setting are more legally vulnerable to trespassers who attack the system.

Therefore, the **Interactive Logon: Message title for users attempting to log on** setting is enabled with suitable text for both of the environments that are discussed in this chapter.

**Note**: Any warning that you display should first be approved by your organization's legal and human resources representatives. Also, the **Interactive logon: Message text for users attempting to log on** and the **Interactive logon: Message title for users attempting to log on** settings must both be enabled for either one to work properly.

## Interactive Logon: Number of previous logons to cache (in case domain controller is not available)

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a domain controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. The default value for this policy setting is 10. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords.

The **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting is configured to **2** for both desktop and laptop computers in the EC environment and for the laptop computers in the SSLF environment. However, this policy setting is configured to **0** for desktops in the SSLF environment because these computers should always be securely connected to the organization’s network.

## Interactive Logon: Prompt user to change password before expiration

This policy setting determines how far in advance users are warned that their password will expire. Microsoft recommends that you configure this policy setting to 14 days to sufficiently warn users when their passwords will expire.

The **Interactive logon: Prompt user to change password before expiration** setting is configured to **14 days** for both of the environments that are discussed in this chapter.

## Interactive Logon: Require Domain Controller authentication to unlock workstation

When this policy setting is enabled, a domain controller must authenticate the domain account used to unlock the computer. When this policy setting is disabled, cached credentials can be used to unlock the computer. Microsoft recommends that this policy setting be disabled for laptop users in both environments, because mobile users do not have network access to domain controllers.

The **Interactive logon: Require Domain Controller authentication to unlock workstation** setting is configured to **Enabled** for desktop computers in both the EC and SSLF environments. However, this policy setting is configured to **Disabled** for laptops in both of the environments, which allows these users to work when they are away from the office.

## Interactive Logon: Smart card removal behavior

This policy setting determines what happens when the smart card for a logged on user is removed from the smart card reader. When configured to **Lock Workstation**, this policy setting locks the workstation when the smart card is removed, which allows users to leave the area, take their smart cards with them, and automatically lock their workstations. If you configure this policy setting to **Force Logoff**, users will be automatically logged off when the smart card is removed.

The **Interactive logon: Smart card removal behavior** setting is configured to the **Lock Workstation** option for both of the environments that are discussed in this chapter.

# *Microsoft Network Client*

The following table summarizes the recommended security option settings for Microsoft network client computers. Additional information is provided in the subsections that follow the table.

**Table 3.10 Security Option Setting Recommendations – Microsoft Network Client**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Microsoft network client: Digitally sign communications (always) | Enabled | Enabled | Enabled | Enabled |
| Microsoft network client: Digitally sign communications (if server agrees) | Enabled | Enabled | Enabled | Enabled |
| Microsoft network client: Send unencrypted password to third-party SMB servers | Disabled | Disabled | Disabled | Disabled |

## Microsoft network client: Digitally sign communications (always)

This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to **Disabled** because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments.

The **Microsoft network client: Digitally sign communications (always)** setting is configured to **Enabled** for computers for both of the environments that are discussed in this chapter.

**Note**: When Windows XP computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, **Microsoft network server: Digitally sign communications (always)**, on those servers. For more details about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available for download at http://go.microsoft.com/fwlink/?LinkId=15159.

## Microsoft network client: Digitally sign communications (if server agrees)

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing. The implementation of digital signing in Windows networks helps to prevent sessions from being hijacked. If you enable this policy setting, the Microsoft network client will use signing only if the server with which it communicates accepts digitally signed communication.

The **Microsoft network client: Digitally sign communications (if server agrees)** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

**Note**: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment.

## Microsoft network client: Send unencrypted password to third-party SMB servers

Disable this policy setting to prevent the SMB redirector from sending plaintext passwords during authentication to non-Microsoft SMB servers that do not support password encryption. Microsoft recommends that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network.

The **Microsoft network client: Send unencrypted password to third-party SMB servers** setting is configured to **Disabled** for the two environments that are discussed in this chapter.

# *Microsoft Network Server*

The following table summarizes the recommended security option settings for Microsoft network servers. Additional information is provided in the subsections that follow the table.

**Table 3.11 Security Option Setting Recommendations – Microsoft Network Server**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Microsoft network server: Amount of idle time required before suspending session | 15 minutes | 15 minutes | 15 minutes | 15 minutes |
| Microsoft network server: Digitally sign communications (always) | Enabled | Enabled | Enabled | Enabled |
| Microsoft network server: Digitally sign communications (if client agrees) | Enabled | Enabled | Enabled | Enabled |

## Microsoft network server: Amount of idle time required before suspending session

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

The **Microsoft network server: Amount of idle time required before suspending session** setting is configured to **Enabled** for a period of **15 minutes** in both of the environments that are discussed in this chapter.

## Microsoft network server: Digitally sign communications (always)

This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server.

The **Microsoft network server: Digitally sign communications (always)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

## Microsoft network server: Digitally sign communications (if client agrees)

This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes

from the client, a connection will be allowed without a signature if the **Microsoft network server: Digitally sign communications (always)** setting is not enabled.

The **Microsoft network server: Digitally sign communications (if client agrees)** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

**Note**: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment.

# Network Access

The following table summarizes the recommended security option settings for network access. Additional information is provided in the subsections that follow the table.

**Table 3.12 Security Option Setting Recommendations – Network Access**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Network access: Allow anonymous SID/Name translation | Disabled | Disabled | Disabled | Disabled |
| Network access: Do not allow anonymous enumeration of SAM accounts | Enabled | Enabled | Enabled | Enabled |
| Network access: Do not allow anonymous enumeration of SAM accounts and shares | Enabled | Enabled | Enabled | Enabled |
| Network access: Do not allow storage of credentials or .NET Passports for network authentication | Enabled | Enabled | Enabled | Enabled |
| Network access: Let Everyone permissions apply to anonymous users | Disabled | Disabled | Disabled | Disabled |
| Network access: Named Pipes that can be accessed anonymously | Not Defined | Not Defined | * See the following setting description for the complete list of named pipes | * See the following setting description for the complete list of named pipes |
| Network access: Remotely accessible registry paths | Not Defined | Not Defined | * See the following setting description for the complete list of paths | * See the following setting description for the complete list of paths |
| Network access: Shares that can be accessed anonymously | Not Defined | Not Defined | comcfg, dfs$ | comcfg, dfs$ |

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Network access: Sharing and security model for local accounts | Classic – local users authenticate as themselves | Classic – local users authenticate as themselves | Classic – local users authenticate as themselves | Classic – local users authenticate as themselves |

## Network access: Allow anonymous SID/Name translation

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding username. Disable this policy setting to prevent unauthenticated users from obtaining usernames that are associated with their respective SIDs.

The **Network access: Allow anonymous SID/Name translation** setting is configured to **Disabled** for the two environments that are discussed in this chapter.

## Network access: Do not allow anonymous enumeration of SAM accounts

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will be not be able to enumerate domain account user names on the workstations in your environment. This policy setting also allows additional restrictions on anonymous connections.

The **Network access: Do not allow anonymous enumeration of SAM accounts** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Network access: Do not allow anonymous enumeration of SAM accounts and shares

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment.

The **Network access: Do not allow anonymous enumeration of SAM accounts and shares** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Network access: Do not allow storage of credentials or .NET Passports for network authentication

This policy setting controls the storage of authentication credentials and passwords on the local system.

The **Network access: Do not allow storage of credentials or .NET Passports for network authentication** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Network access: Let Everyone permissions apply to anonymous users

This policy setting determines what additional permissions are assigned for anonymous connections to the computer. If you enable this policy setting, anonymous Windows users are

allowed to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks.

Therefore, the **Network access: Let Everyone permissions apply to anonymous users** setting is configured to **Disabled** for both of the environments that are discussed in this chapter.

## Network access: Named Pipes that can be accessed anonymously

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

For the EC environment the **Network access: Named Pipes that can be accessed anonymously** setting is configured to **Not Defined**. However, the following default values are enforced for the SSLF environment:

- COMNAP
- COMNODE
- SQL\QUERY
- SPOOLSS
- LLSRPC
- Browser

## Network access: Remotely accessible registry paths

This policy setting determines which registry paths will be accessible after referencing the WinReg key to determine access permissions to the paths.

For the EC environment the **Network access: Remotely accessible registry paths** setting is configured to **Not Defined**. However, for the SSLF environment the following default values are enforced:

- System\CurrentControlSet\Control\ProductOptions
- System\CurrentControlSet\Control\Print\Printers
- System\CurrentControlSet\Control\Server Applications
- System\CurrentControlSet\Control\ContentIndex
- System\CurrentControlSet\Control\Terminal Server
- System\CurrentControlSet\Control\Terminal Server\UserConfig
- System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
- System\CurrentControlSet\Services\Eventlog
- Software\Microsoft\OLAP Server
- Software\Microsoft\Windows NT\CurrentVersion

## Network access: Shares that can be accessed anonymously

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.

The **Network access: Shares that can be accessed anonymously** setting is configured to **Not Defined** for the EC environment. However, ensure that this setting is configured to **comcfg, dfs$** for the SSLF environment.

**Note**: It can be very dangerous to add other shares to this Group Policy setting. Any shares that are listed can be accessed by any network user, which could result in exposure or corruption of sensitive data.

## Network access: Sharing and security model for local accounts

This policy setting determines how network logons that use local accounts are authenticated. The **Classic** option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The **Guest only** option allows you to treat all users equally. In this context, all users authenticate as **Guest only** to receive the same access level to a given resource.

Therefore, the **Sharing and security model for local accounts** setting uses the default **Classic** option for both of the environments that are discussed in this chapter.

# *Network Security*

The following table summarizes the recommended security option settings for network security. Additional information is provided in the subsections that follow the table.

**Table 3.13 Security Option Setting Recommendations – Network Security**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Network security: Do not store LAN Manager hash value on next password change | Enabled | Enabled | Enabled | Enabled |
| Network security: LAN Manager authentication level | Send NTLMv2 responses only\refuse LM | Send NTLMv2 responses only\refuse LM | Send NTLMv2 response only\refuse LM and NTLM | Send NTLMv2 response only\refuse LM and NTLM |
| Network security: LDAP client signing requirements | Negotiate signing | Negotiate signing | Negotiate signing | Negotiate signing |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption |

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption | Require message confidentiality, Require message integrity, Require NTLMv2 session security, Require 128 bit encryption |

## Network security: Do not store LAN Manager hash value on next password change

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Windows NT® hash.

For this reason, the **Network security: Do not store LAN Manager hash value on next password change** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: Very old operating systems and some third-party applications may fail when this policy setting is enabled. Also you will need to change the password on all accounts after you enable this setting.

## Network security: LAN Manager authentication level

This policy setting specifies the type of challenge/response authentication for network logons with non-Windows 2000 and Window XP Professional clients. LAN Manager authentication (LM) is the least secure method; it allows encrypted passwords to be cracked because they can be easily intercepted on the network. NT LAN Manager (NTLM) is somewhat more secure. NTLMv2 is a more robust version of NTLM that is available in Windows XP Professional, Windows 2000, and Windows NT 4.0 Service Pack 4 (SP4) or later. NTLMv2 is also available for Windows 95 and Windows 98 with the optional Directory Services Client.

Microsoft recommends that you configure this policy setting to the strongest possible authentication level for your environment. In environments that run only Windows 2000 Server or Windows Server 2003 with Windows XP Professional workstations, configure this policy setting to the **Send NTLMv2 response only\refuse LM and NTLM** option for the highest security.

The **Network security: LAN Manager authentication level** setting is configured to **Send NTLMv2 response only\refuse LM** for the EC environment. However, this policy setting is configured to the more restrictive **Send NTLMv2 response only\refuse LM and NTLM** for the SSLF environment.

## Network security: LDAP client signing requirements

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests. Because unsigned network traffic is susceptible to man-in-the-middle attacks, an attacker could cause an LDAP server to make decisions that are based on false queries from the LDAP client.

Therefore, the value for the **Network security: LDAP client signing requirements** setting is configured to **Negotiate signing** for both of the environments that are discussed in this chapter.

## Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

This policy setting determines the minimum application-to-application communications security standards for clients. The options for this policy setting are:

- Require message integrity
- Require message confidentiality
- Require NTLMv2 session security
- Require 128-bit encryption

If all of the computers on your network can support NTLMv2 and 128-bit encryption (for example, Windows XP Professional SP2 and Windows Server 2003 SP1), all four setting options may be selected for maximum security.

All four options are enabled for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** setting in both of the environments that are discussed in this chapter.

## Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

This policy setting is similar to the previous setting, but affects the server side of communication with applications. The options for the setting are the same:

- Require message integrity
- Require message confidentiality
- Require NTLMv2 session security
- Require 128-bit encryption

If all of the computers on your network can support NTLMv2 and 128-bit encryption (for example, Windows XP Professional SP2 and Windows Server 2003 SP1), all four options may be selected for maximum security.

All four options are enabled for the **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** setting in both of the environments that are discussed in this chapter.

# *Recovery Console*

The following table summarizes the recommended security option settings for the recovery console. Additional information is provided in the subsections that follow the table.

**Table 3.14 Security Option Setting Recommendations – Recovery Console**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Recovery console: Allow automatic administrative logon | Disabled | Disabled | Disabled | Disabled |
| Recovery console: Allow floppy copy and access to all drives and all folders | Not Defined | Not Defined | Disabled | Disabled |

## Recovery console: Allow automatic administrative logon

The recovery console is a command-line environment that is used to recover from system problems. If you enable this policy setting, the administrator account is automatically logged on to the recovery console when it is invoked during startup. Microsoft recommends that you disable this policy setting, which will require administrators to enter a password to access the recovery console.

The **Recovery console: Allow automatic administrative logon** setting is configured to **Disabled** for the two environments that are discussed in this chapter.

## Recovery console: Allow floppy copy and access to all drives and all folders

This policy setting makes the Recovery Console SET command available, which allows you to set the following recovery console environment variables:

- **AllowWildCards**. Enables wildcard support for some commands (such as the DEL command).
- **AllowAllPaths**. Allows access to all files and folders on the computer.
- **AllowRemovableMedia**. Allows files to be copied to removable media, such as a floppy disk.
- **NoCopyPrompt**. Does not prompt when overwriting an existing file.

The **Recovery console: Allow floppy copy and access to all drives and all folders** setting is configured to **Not Defined** for the EC environment. However, for maximum security, this setting is configured to **Disabled** for the SSLF environment.

# *Shutdown*

The following table summarizes shutdown security option setting recommendations. Additional information is provided in the subsections that follow the table.

**Table 3.15 Security Option Setting Recommendations – Shutdown**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Shutdown: Allow system to be shut down without having to log on | Not Defined | Not Defined | Disabled | Disabled |
| Shutdown: Clear virtual memory pagefile | Disabled | Disabled | Disabled | Disabled |

## Shutdown: Allow system to be shut down without having to log on

This policy setting determines whether a computer can be shut down when a user is not logged on to it. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. Microsoft recommends that you disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system.

The **Shutdown: Allow system to be shut down without having to log on** setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Shutdown: Clear virtual memory pagefile

This policy setting determines whether the virtual memory pagefile is cleared when the system is shut down. When this policy setting is enabled, the system pagefile is cleared each time that the system shuts down gracefully. If you enable this security setting, the hibernation file (Hiberfil.sys) is also zeroed out when hibernation is disabled on a portable computer system. It will take longer to shut down and restart the server, and will be especially noticeable on servers with large paging files.

For these reasons, the **Shutdown: Clear virtual memory pagefile** setting is configured to **Disabled** for all computer types in both of the environments that are discussed in this chapter.

# *System Cryptography*

The following table summarizes the recommended security option settings for system cryptography. Additional information is provided after the table.

**Table 3.16 Security Option Setting Recommendations – System Cryptography**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing | Not Defined | Not Defined | Disabled | Disabled |

## System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

This policy setting determines whether the Transport Layer Security/Secure Sockets Layer (TL/SS) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Although this policy setting increases security, most public Web sites that are secured with TLS or SSL do not support these algorithms. Client computers that have this policy setting enabled will also be unable to connect to Terminal Services on servers that are not configured to use the FIPS compliant algorithms.

The **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

**Note**: If you enable this policy setting, computer performance will be slower because the 3DES process is performed on each block of data in the file three times. This policy setting should only be enabled if your organization is required to be FIPS compliant.

# System Objects

The following table summarizes the recommended security option settings for system objects. Additional information is provided in the subsections that follow the table.

**Table 3.17 Security Option Setting Recommendations – System Objects**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| System objects: Default owner for objects created by members of the Administrators group | Object Creator | Object Creator | Object Creator | Object Creator |
| System objects: Require case insensitivity for non-Windows subsystems | Not Defined | Not Defined | Enabled | Enabled |
| System objects: Strengthen default permissions of internal system objects | Enabled | Enabled | Enabled | Enabled |

## System objects: Default owner for objects created by members of the Administrators group

This policy setting determines whether the **Administrators** group or the **Object Creator** group is the default owner of new system objects.

To provide greater accountability, the **System objects: Default owner for objects created by members of the Administrators group** setting is configured to the **Object Creator** group for the two environments that are discussed in this chapter.

## System objects: Require case insensitivity for non-Windows subsystems

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32® subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation may block access to these files by another user who uses typical Win32 tools, because only one of the files will be available.

To ensure consistency of file names, the **System objects: Require case insensitivity for non-Windows subsystems** setting is configured to **Not Defined** for the EC environment and to **Enabled** for the SSLF environment.

## System objects: Strengthen default permissions of internal system objects

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. The setting helps secure objects that can be located and shared among processes and its default configuration strengthens the DACL, because it allows users who are not administrators to read shared objects but does not allow them to modify any that they did not create.

Therefore, the **System objects: Strengthen default permissions of internal system objects** (for example, Symbolic Links) setting is configured to the default setting of **Enabled** for both of the environments that are discussed in this chapter.

# Event Log Security Settings

The event log records events on the system, and the Security log records audit events. The event log container of Group Policy is used to define attributes that are related to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. The settings for the Application, Security, and System event logs are configured in the member server baseline policy (MSBP) and applied to all member servers in the domain.

You can configure the event log settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\Event Log**

This section provides details about the prescribed settings for the environments that are discussed in this chapter. For a summary of the prescribed settings in this section, see the Microsoft Excel® workbook "Windows XP Security Guide Settings." For information about the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at http://go.microsoft.com/fwlink/?LinkId=15159. The companion guide also includes detailed information about the potential for lost event log data when the log sizes are set to very large values.

The following table summarizes the recommended event log security settings for both desktop and laptop clients in the two types of environments that are discussed in this chapter—the Enterprise Client (EC) environment and the Specialized Security – Limited Functionality (SSLF) environment. More detailed information about each of the settings is provided in the following subsections.

**Table 3.18 Event Log Security Setting Recommendations**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Maximum application log size | 16384 KB | 16384 KB | 16384 KB | 16384 KB |
| Maximum security log size | 81920 KB | 81920 KB | 81920 KB | 81920 KB |
| Maximum system log size | 16384 KB | 16384 KB | 16384 KB | 16384 KB |
| Prevent local guests group from accessing application log | Enabled | Enabled | Enabled | Enabled |
| Prevent local guests group from accessing security log | Enabled | Enabled | Enabled | Enabled |
| Prevent local guests group from accessing system log | Enabled | Enabled | Enabled | Enabled |
| Retention method for application log | As Needed | As Needed | As Needed | As Needed |
| Retention method for security log | As Needed | As Needed | As Needed | As Needed |
| Retention method for system log | As Needed | As Needed | As Needed | As Needed |

## *Maximum application log size*

This policy setting specifies the maximum size of the Application event log, which has a maximum capacity of 4 GB. However, this size is not recommended because of the risk of memory fragmentation, which causes slow performance and unreliable event logging. Requirements for

the Application log size vary, and depend on the function of the platform and the need for historical records of application-related events.

The **Maximum application log size** setting is configured to **16384 KB** for all computers in the two environments that are discussed in this chapter.

## Maximum security log size

This policy setting specifies the maximum size of the Security event log, which has a maximum capacity of 4 GB. However, this size is not recommended because of the risk of memory fragmentation, which causes slow performance and unreliable event logging. Requirements for the Security log size vary, and depend on the function of the platform and the need for historical records of application-related events.

The **Maximum security log size** setting is configured to **81920 KB** for all computers in the two environments that are discussed in this chapter.

## Maximum system log size

This policy setting specifies the maximum size of the System event log, which has a maximum capacity of 4 GB. However, this size is not recommended because of the risk of memory fragmentation, which leads to slow performance and unreliable event logging. Requirements for the application log size vary depending on the function of the platform and the need for historical records of application related events.

The **Maximum system log size** setting is configured to **16384 KB** for all computers in the two environments that are discussed in this chapter.

## Prevent local guests group from accessing application log

This policy setting determines whether guests are prevented from accessing the Application event log. By default in Windows Server 2003, guest access is prohibited on all systems. Therefore, this policy setting has no real effect on default system configurations. However, it is considered a defense-in-depth setting with no side effects.

The **Prevent local guests group from accessing application log** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Prevent local guests group from accessing security log

This policy setting determines whether guests are prevented from accessing the Security event log. A user must be assigned the **Manage auditing and security log** user right (not defined in this guidance) to access the Security log. Therefore, this policy setting has no real effect on default system configurations. However, it is considered a defense-in-depth setting with no side effects.

The **Prevent local guests group from accessing security log** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Prevent local guests group from accessing system log

This policy setting determines whether guests are prevented from accessing the System event log. By default in Windows Server 2003, guest access is prohibited on all systems. Therefore, this policy setting has no real effect on default system configurations. However, it is considered a defense-in-depth setting with no side effects.

The **Prevent local guests group from accessing system log** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Retention method for application log

This policy setting determines the "wrapping" method for the Application log. It is imperative that the Application log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this configuration could result in a loss of historical data.

The **Retention method for application log** is configured to **As Needed** for both of the environments that are discussed in this chapter.

## Retention method for security log

This policy setting determines the "wrapping" method for the Security log. It is imperative that the Security log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this configuration could result in a loss of historical data.

The **Retention method for security log** is configured to **As Needed** for both of the environments that are discussed in this chapter.

## Retention method for system log

This policy setting determines the "wrapping" method for the System log. It is imperative that the System log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this configuration could result in a loss of historical data.

The **Retention method for system log** is configured to **As Needed** for both of the environments that are discussed in this chapter.

# Restricted Groups

The Restricted Groups setting allows you to manage the membership of groups in Windows XP Professional through Active Directory Group Policy. First, review the needs of your organization to determine the groups you want to restrict. For this guidance, the **Backup Operators** and **Power Users** groups are restricted in both of the environments but only the **Remote Desktop Users** group is restricted for the SSLF environment. Although members of the **Backup Operators** and **Power Users** groups have less system access than members in the **Administrators** group, they can still access the system in powerful ways.

**Note:** If your organization uses any of these groups, then carefully control their membership and do not implement the guidance for the Restricted Groups setting. If your organization adds users to the Power Users group, you may want to implement the optional file system permissions that are described in the "Securing the File System" section later in this chapter.

**Table 3.19 Restricted Groups Recommendations**

| Local group | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Backup Operators | No members | No members | No members | No members |
| Power Users | No members | No members | No members | No members |
| Remote Desktop Users | | | No members | No members |

You can configure the Restricted Groups setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\Restricted Groups**

Administrators may configure restricted groups for a GPO by adding the desired group directly to the **Restricted Groups** node of the GPO namespace.

When a group is restricted, you can define its members and any other groups to which it belongs. If you do not specify these group members, the group is left totally restricted. Groups can only be restricted by using security templates.

**To view or modify the Restricted Groups setting**

1. Open the Security Templates Management Console.

   **Note**: The Security Templates Management Console is not added to the Administrative Tools menu by default. To add it, start the Microsoft Management Console (mmc.exe) and add the Security Templates Add-in.

2. Double-click the configuration file directory, and then the configuration file.
3. Double-click the **Restricted Groups** item.
4. Right-click **Restricted Groups** and then select **Add Group**.
5. Click the **Browse** button, the **Locations** button, select the locations you want to browse, and then click **OK**.

   **Note**: Typically, this will result in a local computer appearing at the top of the list.

6. Type the group name in the **Enter the object names to select** text box and then click the **Check Names** button.

   – Or –

   Click the **Advanced** button, and then the **Find Now** button to list all available groups.

7. Select the groups you want to restrict, and then click **OK**.
8. Click **OK** on the **Add Groups** dialog box to close it.

In this guidance, the settings were removed for all members—users and groups—of the Power Users and Backup Operators groups to totally restrict them in both environments. Also, for the SSLF environment, all members were removed for the Remote Desktop Users group. Microsoft recommends that you restrict any built-in group you do not plan to use in your organization.

**Note**: The configuration of Restricted Groups that is described in this section is very simple. Versions of Windows XP SP1 or later, as well as Windows Server 2003, support more complex designs. For more information, see the Microsoft Knowledge Base article "Updates to Restricted Groups ("Member of") Behavior of User-Defined Local Groups" at http://support.microsoft.com/default.aspx?kbid=810076.

# System Services

When Windows XP Professional is installed, default system services are created and configured to run when the system starts. Many of these system services do not need to run in the environments that are discussed in this chapter.

There are additional optional services available with Windows XP Professional, such as IIS, that are not installed during the default installation of the operating system. You can add these optional services to an existing system through Add/Remove Programs in Control Panel, or you can create a customized automated installation of Windows XP Professional.

**Important**: Remember that any service or application is a potential point of attack. Therefore, any unneeded services or executable files should be disabled or removed in your environment.

You can configure the system services settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\System Services**

An administrator can set the startup mode of the system services and change the security settings for each of them.

**Important**: Versions of the graphical tools that can be used to edit services that were included with pre-Windows 2003 versions of the Windows operating system automatically apply permissions to each service when you configure any of the properties of a service. Tools such as the Group Policy Object Editor and the MMC Security Templates snap-in use the Security Configuration Editor DLL to apply these permissions. If the default permissions are changed, a variety of problems will occur for many services. Microsoft recommends that you not alter the permissions on services that are included with Windows XP or Windows Server 2003, because the default permissions are already quite restrictive.

The Windows Server 2003 version of the Security Configuration Editor DLL does not force you to configure permissions when you edit the properties of a service. For more information see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

The following table summarizes the recommended system services settings for both desktop and laptop clients in the two types of environments that are discussed in this chapter—the Enterprise Client (EC) environment and the Specialized Security – Limited Functionality (SSLF) environment. More detailed information about each of the settings is provided in the following subsections.

**Table 3.20 System Services Security Setting Recommendations**

| Service name | Display name | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|---|
| Alerter | Alerter | Disabled | Disabled | Disabled | Disabled |
| ClipSrv | ClipBook | Disabled | Disabled | Disabled | Disabled |
| Browser | Computer Browser | Not Defined | Not Defined | Disabled | Disabled |
| Fax | Fax | Not Defined | Not Defined | Disabled | Disabled |
| MSFtpsvr | FTP Publishing | Disabled | Disabled | Disabled | Disabled |
| IISADMIN | IIS Admin | Disabled | Disabled | Disabled | Disabled |
| cisvc | Indexing Service | Not Defined | Not Defined | Disabled | Disabled |
| Messenger | Messenger | Disabled | Disabled | Disabled | Disabled |
| mnmsrvc | NetMeeting® Remote Desktop Sharing | Disabled | Disabled | Disabled | Disabled |
| RDSessMgr | Remote Desktop Help Session Manager | Not Defined | Not Defined | Disabled | Disabled |
| RemoteAccess | Routing and Remote Access | Disabled | Disabled | Disabled | Disabled |

| Service name | Display name | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|---|
| SNMP | SNMP Service | Disabled | Disabled | Disabled | Disabled |
| SNMPTRAP | SNMP Trap Service | Disabled | Disabled | Disabled | Disabled |
| SSDPSrv | SSDP Discovery Service | Disabled | Disabled | Disabled | Disabled |
| Schedule | Task Scheduler | Not Defined | Not Defined | Disabled | Disabled |
| TlntSvr | Telnet | Disabled | Disabled | Disabled | Disabled |
| TermService | Terminal Services | Not Defined | Not Defined | Disabled | Disabled |
| Upnphost | Universal Plug and Play Device Host | Not Defined | Not Defined | Disabled | Disabled |
| W3SVC | World Wide Web Publishing | Disabled | Disabled | Disabled | Disabled |

## Alerter

This service notifies selected users and computers of administrative alerts. You can use this service to send alert messages to specified users who are connected to your network.

The **Alerter** service is configured to **Disabled** to prevent information from being sent across the network. This configuration ensures greater security for the two environments that are discussed in this chapter.

**Note**: The functionality of uninterruptible power supply (UPS) alert message systems can be affected if you disable this service.

## ClipBook

This service allows the Clipbook Viewer to create and share “pages” of data that may be viewed by remote computers. The service depends on the Network Dynamic Data Exchange (NetDDE) service to create the actual file shares that other computers can connect to; the **Clipbook** application and service allow you to create the pages of data to share. Any services that explicitly depend on this service will fail. However, you can use Clipbrd.exe to view the local clipboard, which is where data is stored when a user selects text and then clicks **Copy** on the **Edit** menu or presses CTRL+C.

The **ClipBook** service is configured to **Disabled** to ensure greater security for the two environments that are discussed in this chapter.

## Computer Browser

This service maintains an up-to-date list of computers on your network and supplies the list to programs that request it. The service is used by Windows-based computers that need to view network domains and resources.

To ensure greater security, the **Computer Browser** service is set to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Fax

This service is a Telephony API (TAPI)-compliant service that provides fax capabilities on the clients in your environment. The service allows users to send and receive faxes from their desktop applications through either a local fax device or a shared network fax device.

The **Fax** service is configured to **Not Defined** for the computers in the EC environment. However, this service is set to **Disabled** for the SSLF environment to ensure greater security.

## FTP Publishing

This service provides connectivity and administration through the MMC IIS snap-in. Microsoft recommends that you not install this service on Windows XP clients in your environment unless there is a business need for the service.

The **FTP Publishing** service is configured to **Disabled** for the two environments that are discussed in this chapter.

## IIS Admin

This service allows administration of IIS components, such as FTP, Applications Pools, Web sites, and Web service extensions. Disable this service to prevent users from running Web or FTP sites on their computers, which are not needed on most Windows XP client computers.

The **IIS Admin** service is configured to **Disabled** for the two environments that are discussed in this chapter.

## Indexing Service

This service indexes the contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language. The service also enables you to “quick search” documents on local and remote computers and provides a search index for content that is shared on the Web.

The **Indexing Service** is configured to **Not Defined** for the computers in the EC environment. However, this service is set to **Disabled** for the SSLF environment to ensure greater security.

## Messenger

This service transmits and sends **Alerter** service messages between clients and servers. This service is not related to Windows Messenger or MSN Messenger, and is not a requirement for Windows XP client computers.

For this reason, the **Messenger** service is configured to **Disabled** for the two environments that are discussed in this chapter.

## NetMeeting Remote Desktop Sharing

This service allows an authorized user to access a client remotely through Microsoft NetMeeting over an organization’s intranet. This service must be explicitly enabled in NetMeeting. You can also disable this feature in NetMeeting, shut down the service by means of a Windows tray icon, or disable this feature in Group Policy by configuring the **Disable Remote Desktop Sharing** setting, which is discussed in Chapter 4, "Administrative Templates for Windows XP." Microsoft recommends that you disable this service to prevent access to your clients from remote locations.

The **NetMeeting Remote Desktop Sharing** service is configured to **Disabled** for the two environments that are discussed in this chapter.

## Remote Desktop Help Session Manager

This service manages and controls the Remote Assistance feature in the Help and Support Center application (Helpctr.exe).

The **Remote Desktop Help Session Manager** service is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Routing and Remote Access

This service provides multi-protocol LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services. This service also provides dial-up and VPN remote access services.

The **Routing and Remote Access** service is configured to **Disabled** for both of the environments that are discussed in this chapter.

## SNMP Service

This service allows incoming Simple Network Management Protocol (SNMP) requests to be serviced by the local computer. **SNMP Service** includes agents that monitor activity in network devices and report to the network console workstation.

The **SNMP Service** is configured to **Disabled** for both of the environments that are discussed in this chapter.

## SNMP Trap Service

This service receives trap messages that are generated by local or remote SNMP agents and forwards the messages to SNMP management programs that run on your computer. The **SNMP Service**, when configured for an agent, generates trap messages if any specific events occur. These messages are sent to a trap destination.

The **SNMP Trap Service** is configured to **Disabled** for both of the environments that are discussed in this chapter.

## SSDP Discovery Service

This service provides the Universal Plug and Play host service with the ability to locate and identify UPnP network devices. If you disable the **SSDP Discovery Service**, the system will be prevented from finding UPnP devices on the network and the Universal Plug and Play host service will fail to find and interact with UPnP devices.

The **SSDP Discovery Service** is configured to **Disabled** for both of the environments that are discussed in this chapter.

## Task Scheduler

This service enables you to configure and schedule automated tasks on your computer. The service monitors whatever criteria you choose and carries out the task when the criteria have been met.

The **Task Scheduler** service is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Telnet

This service for Windows provides ASCII terminal sessions to Telnet clients. The service supports two types of authentication and the following four types of terminals: ANSI, VT-100, VT-52, and VTNT. However, this service is not a requirement for most Windows XP clients.

The **Telnet** service is configured to **Disabled** for the two environments that are discussed in this chapter.

## Terminal Services

This service provides a multi-session environment that allows client devices to access a virtual Windows desktop session and Windows-based programs that run on the server. In Windows XP, this service allows remote users to be connected interactively to a computer and to display desktops and applications on remote computers.

The **Terminal Services** service is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## Universal Plug and Play Host

This service supports peer-to-peer Plug and Play functionality for network devices. The UPnP specification is designed to simplify device and network service installation and management. UPnP accomplishes device and service discovery and control through driver-less, standards-based protocol mechanisms. Universal Plug and Play devices can auto-configure network addressing, announce their presence on a network subnet, and enable the exchange of device and service descriptions. A Windows XP computer can act as a UPnP control point to discover and control the devices through a Web or application interface.

The **Universal Plug and Play** service is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## World Wide Web Publishing

This service provides Web connectivity and administration through the MMC IIS snap-in. The service provides HTTP services for applications on the Windows platform and contains a process manager and a configuration manager. However, this service is not a requirement for most Windows XP clients.

The **World Wide Web Publishing** service is configured to **Disabled** for the two environments that are discussed in this chapter.

# Additional Registry Settings

Additional registry value entries were created for the baseline security template files that are not defined within the Administrative Template (.adm) file for both of the security environments that are discussed in this chapter.

These settings are embedded within the security templates (in the “Security Options” section) to automate their implementation. If the policy is removed, these settings are not automatically removed with it; they must be manually changed with a registry editing tool such as Regedt32.exe.

This guide includes additional settings that are added to the Security Configuration Editor (SCE) by modifying the Sceregvl.inf file (located in the **%windir%\inf** folder) and re-registering the Scecli.dll file. The original security settings as well as the additional ones appear under **Local**

**Policies\Security Options** in the snap-ins and tools that are listed earlier in this chapter. You should update the Sceregvl.inf file and re-register Secli.dll as described in the subsection "How to Modify the Security Configuration Editor User Interface" that follows this one for any computers that require you to edit the security templates and Group Policies that are provided with this guide.

The following table summarizes the additional registry setting recommendations for both desktop and laptop clients in the two types of environments that are discussed in this chapter—the Enterprise Client (EC) environment and the Specialized Security – Limited Functionality (SSLF) environment.

Additional information about each of the settings is provided in the subsections that follow the table. For information about the default settings and a detailed explanation of each of the settings, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

**Table 3.21 Additional Registry Settings**

| Setting name | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) | Not defined | Not defined | Disabled | Disabled |
| MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | Not defined | Not defined | Highest Protection, source routing is completely disabled. | Highest Protection, source routing is completely disabled. |
| MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS) | Not defined | Not defined | Disabled | Disabled |
| MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | Not defined | Not defined | Disabled | Disabled |
| MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | Not defined | Not defined | Enabled | Enabled |
| MSS: (KeepAliveTime)How often keep-alive packets are sent in milliseconds | Not defined | Not defined | 30000 or 5 minutes (recommend ed) | 30000 or 5 minutes (recommend ed) |
| MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended) | Multicast, broadcast, and ISAKMP are exempt (Best for Windows XP) | Multicast, broadcast, and ISAKMP are exempt (Best for Windows XP) | Multicast, broadcast, and ISAKMP are exempt (Best for Windows XP) | Multicast, broadcast, and ISAKMP are exempt (Best for Windows XP) |
| MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended) | 255, disable autorun for all drives | 255, disable autorun for all drives | 255, disable autorun for all drives | 255, disable autorun for all drives |

| Setting name | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | Not defined | Not defined | Enabled | Enabled |
| MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended) | Not defined | Not defined | Enabled | Enabled |
| MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | Not defined | Not defined | Enabled | Enabled |
| MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) | Enabled | Enabled | Enabled | Enabled |
| MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | 0 | 0 | 0 | 0 |
| MSS: (SynAttackProtect) Syn attack protection level (protects against DoS) | Not defined | Not defined | Connections timeout sooner if attack is detected | Connections timeout sooner if attack is detected |
| MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged | Not defined | Not defined | 3 & 6 seconds, half-open connections dropped after 21 seconds | 3 & 6 seconds, half-open connections dropped after 21 seconds |
| MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | Not defined | Not defined | 3 | 3 |
| MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | Not defined | Not defined | 90 | 90 |

# (AutoAdminLogon) Enable Automatic Logon

The registry value entry **AutoAdminLogon** was added to the template file in the **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon** registry key. The entry appears as **MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)** in the SCE.

This setting is separate from the **Welcome** screen feature in Windows XP; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the **Authenticated Users** group. For these reasons the setting is configured to **Not Defined** for the EC environment, and the default **Disabled** setting is explicitly enforced for the SSLF environment.

For additional information, see the Microsoft Knowledge Base article "How to turn on automatic logon in Windows XP," which is available online at http://support.microsoft.com/default.aspx?scid=315231.

# (DisableIPSourceRouting) IP source routing protection level

The registry value entry **DisableIPSourceRouting** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)** in the SCE.

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. This setting is configured to **Not Defined** for the EC environment and to **Highest Protection, source routing is completely disabled** for the SSLF environment.

# (EnableDeadGWDetect) Allow automatic detection of dead network gateways

The registry value entry **EnableDeadGWDetect** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)** in the SCE.

When dead gateway detection is enabled, the IP may change to a backup gateway if a number of connections experience difficulty. This setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

# (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

The registry value entry **EnableICMPRedirect** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes** in the SCE.

Internet Control Message Protocol (ICMP) redirects cause the stack to plumb host routes. These routes override the Open Shortest Path First (OSPF)-generated routes. This setting is configured to **Not Defined** for the EC environment and to **Disabled** for the SSLF environment.

## (Hidden) Hide the Computer from Network Neighborhood Browse Lists

The registry value entry **Hidden** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters** registry key. The entry appears as **MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)** in the SCE.

You can configure a computer so that it does not send announcements to browsers on the domain. If you do so, you hide the computer from the Browse list, which means that the computer will stop announcing itself to other computers on the same network. An attacker who knows the name of a computer can more easily gather additional information about the system. You can enable this setting to remove one method that an attacker might use to gather information about computers on the network. Also, this setting can help reduce network traffic when enabled. However, the security benefits of this setting are small because attackers can use alternative methods to identify and locate potential targets. For this reason, Microsoft recommends that you enable this setting only in high security environments.

This setting is configured to **Not Defined** for the EC environment and to **Enabled** for the SSLF environment.

For additional information, see the Microsoft Knowledge Base article "HOW TO: Hide a Windows 2000-Based Computer from the Browser List," which is available online at http://support.microsoft.com/default.aspx?scid=321710.

## (KeepAliveTime) How often keep-alive packets are sent in milliseconds

The registry value entry **KeepAliveTime** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds (300,000 is recommended)** in the SCE.

This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet. This setting is configured to **Not Defined** for the EC environment and to **30000 or 5 minutes** for the SSLF environment.

## (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering

The registry value entry **NoDefaultExempt** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC** registry key. The entry appears as **MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)** in the SCE.

The default exemptions to IPsec policy filters are documented in the Microsoft Windows 2000 and Windows XP online help. These filters make it possible for Internet Key Exchange (IKE) and the Kerberos authentication protocol to function. The filters also make it possible for the network Quality of Service (QoS) to be signaled (RSVP) when the data traffic is secured by IPsec, and for traffic that IPsec might not secure such as multicast and broadcast traffic.

IPsec is increasingly used for basic host-firewall packet filtering, particularly in Internet-exposed scenarios, and the affect of these default exemptions has not been fully understood. Therefore, some IPsec administrators may create IPsec policies that they think are secure, but are not actually secure against inbound attacks that use the default exemptions. Microsoft recommends that you enforce the default setting in Windows XP with SP 2, **Multicast, broadcast, and ISAKMP are exempt**, for both of the environments that are discussed in this chapter.

For additional information, see the Microsoft Knowledge Base article "IPSec Default Exemptions Can Be Used to Bypass IPsec Protection in Some Scenarios," which is available online at http://support.microsoft.com/default.aspx?scid=811832.

## *(NoDriveTypeAutoRun) Disable Autorun for all drives*

The registry value entry **NoDriveTypeAutoRun** was added to the template file in the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer** registry key. The entry appears as **MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)** in the SCE.

Autorun starts to read from a drive on your computer as soon as media is inserted into it. As a result, the setup file of programs and the sound on audio media starts immediately. This setting is configured to **255, disable autorun for all drives** for both of the environments that are discussed in this chapter.

## *(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers*

The registry value entry **NoNameReleaseOnDemand** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters** registry key. The entry appears as **MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers** in the SCE.

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows–based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. It is set to **Not Defined** for the EC environment and **Enabled** for the SSLF environment.

## *(NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames*

The registry value entry **NtfsDisable8dot3NameCreation** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem** registry key. The entry appears as **MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)** in the SCE.

Windows Server 2003 supports 8.3 file name formats for backward compatibility with16-bit applications. The 8.3 file name convention is a naming format that allows file names up to eight characters long. This setting is configured to **Not Defined** for the EC environment and to **Enabled** for the SSLF environment.

# (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses

The registry value entry **PerformRouterDiscovery** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)** in the SCE.

This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis. This setting is configured to **Not Defined** for the EC environment and to **Enabled** for the SSLF environment.

# (SafeDllSearchMode) Enable Safe DLL Search Order

The registry value entry **SafeDllSearchMode** was added to the template file in the **HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager** registry key. The entry appears as **MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)** in the SCE.

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways:

- Search folders specified in the system path first, and then search the current working folder.
- Search current working folder first, and then search the folders specified in the system path.

When enabled, the registry value is set to **1**. With a setting of **1**, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to **0** and the system first searches the current working folder and then searches the folders that are specified in the system path. This setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

# (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires

The registry value entry **ScreenSaverGracePeriod** was added to the template file in the **HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon** registry key. The entry appears as **MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)** in the SCE.

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. This setting is configured to **0** seconds for both of the environments that are discussed in this chapter.

# (SynAttackProtect) Syn attack protection level

The registry value entry **SynAttackProtect** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)** in the SCE.

This setting causes TCP to adjust retransmission of SYN-ACKs. When you configure this value, the connection responses time out more quickly if a connect request (SYN) attack is detected.

This setting is configured to **Not Defined** for the EC environment and to **Connections timeout sooner if attack is detected** for the SSLF environment.

## *(TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged*

The registry value entry **TCPMaxConnectResponseRetransmissions** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged** in the SCE.

This setting determines the number of times that TCP retransmits a SYN before the attempt to connect is aborted. The retransmission time-out is doubled with each successive retransmission in a given connect attempt. The initial time-out value is three seconds. This setting is configured to **Not Defined** for the EC environment and to **3 & 6 seconds, half-open connections dropped after 21 seconds** for the SSLF environment.

## *(TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted*

The registry value entry **TCPMaxDataRetransmissions** was added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key. The entry appears as **MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)** in the SCE.

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. This setting is configured to **Not Defined** for the EC environment and to **3** for the SSLF environment.

## *(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning*

The registry value entry **WarningLevel** was added to the template file in the **HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog\Security** registry key. The entry appears as **MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning** in the SCE.

This setting became available with SP3 for Windows 2000, and is a new feature that can generate a security audit in the Security event log when the log reaches a user-defined threshold. This setting is configured to **Not Defined** for the EC environment and to **90** for the SSLF environment.

**Note**: If log settings are configured to **Overwrite events as needed** or **Overwrite events older than x days**, this event will not be generated.

# How to Modify the Security Configuration Editor User Interface

The Security Configuration Editor (SCE) set of tools is used to define security templates that can be applied to individual computers or any number of computers through Group Policy. Security templates can contain password policies, lockout policies, Kerberos authentication protocol policies, audit policies, event log settings, registry values, service startup modes, service permissions, user rights, group membership restrictions, registry permissions, and file system permissions. The SCE appears in a number of MMC snap-ins and administrator tools. It is used by the Security Templates snap-in and the Security Configuration and Analysis snap-in. The Group Policy Object Editor snap-in uses it for the Security Settings portion of the Computer Configuration tree, and it is also used for the Local Security Settings, Domain Controller Security Policy, and the Domain Security Policy tools.

This guide includes additional settings that are added to the SCE. To add these settings, you need to modify the Sceregvl.inf file, which is located in the **%systemroot%\inf** folder, and then re-register the Scecli.dll file.

**Important**: The customized version of the Sceregvl.inf file that is created by the following procedures uses features that are only available in Windows XP Professional with SP 2 and Windows Server 2003. Do not try to install the customized file on older versions of Windows.

After the Sceregvl.inf file is modified and registered, the custom registry values are exposed in the SCE user interfaces on that computer. You will see the new settings at the bottom of the list of items in the SCE—they are all preceded by the text "MSS:" MSS stands for Microsoft Solutions for Security, the name of the group that created this guide. You can then create security templates or policies that define these new registry values and that can be applied to any computer, regardless of whether the Sceregvl.inf file was modified on the target computer or not. Subsequent launches of the SCE will expose your custom registry values.

A number of the new settings that will appear in the SCE are not documented in this guide because they are typically not configured for end-user systems. For further information about these new settings you can refer to the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available for download at http://go.microsoft.com/fwlink/?LinkId=15159.

Instructions about how to modify the SCE user interface are provided in the following procedures. There are manual instructions that you should follow if you have already made other customizations to the SCE. A script is provided to add the settings with little user interaction, and although the script has built-in error detection and recovery features it may fail. If it does fail, you should determine the cause of the failure and either correct the problem or follow the manual instructions. Another script is provided that you can use to restore the SCE user interface to its default state. This script will remove all custom settings and return the SCE to the way it appears in a default installation of Windows XP with SP2 or Windows Server 2003 with SP1.

**To manually update Sceregvl.inf**

1. Use a text editor such as Notepad to open the **Values-sceregvl.txt** file from the **SCE Update** folder of the download for this guide.
2. Open another window in the text editor and then open the **%systemroot%\inf\sceregvl.inf** file.
3. Navigate to the bottom of the “[Register Registry Values]” section in the **sceregvl.inf** file. Copy and paste the text from the **Values-sceregvl.txt** file, without any page breaks, into this section of the **sceregvl.inf** file.
4. Close the **Values-sceregvl.txt** file and open the **Strings-sceregvl.txt** file from the **SCE Update** folder of the download.

5. Navigate to the bottom of the "[Strings]" section in the **sceregvl.inf** file. Copy and paste the text from the **Strings-sceregvl.txt** file, without any page breaks, into this section of the **sceregvl.inf** file.
6. Save the **sceregvl.inf** file and close the text editor.
7. Open a command prompt and execute the command **regsvr32 scecli.dll** to re-register the DLL file.

Subsequent launches of the SCE will display these custom registry values.

**To automatically update sceregvl.inf**

1. The **Values-sceregvl.txt, Strings-sceregvl.txt,** and **Update_SCE_with_MSS_Regkeys.vbs** files that are located in the **SCE Update** folder of the download for this guide must all be in the same location for the script to function.
2. Execute the **Update_SCE_with_MSS_Regkeys.vbs** script on the computer you wish to update.
3. Follow the onscreen prompts.

This procedure will remove only the custom entries that were made with the script that is described in the previous procedure, **Update_SCE_with_MSS_Regkeys.vbs**.

**To reverse the changes made by the Update_SCE_with_MSS_Regkeys.vbs script**

1. Execute the **Rollback_SCE_for_MSS_Regkeys.vbs** script on the computer you wish to update.
2. Follow the onscreen prompts.

This procedure will remove *any* custom entries that you may have added to the SCE user interface, including those from this guide and others that may have been provided in earlier versions of this guide or in other security guides.

**To restore the SCE to its default state for Windows XP with SP2 or Windows Server 2003 with SP1**

1. The **sceregvl_W2K3_SP1.inf.txt, sceregvl_XPSP2.inf.txt,** and **Restore_SCE_to_Default.vbs** files that are located in the **SCE Update** folder of the download for this guide must all be in the same location for the script to function.
2. Execute the **Restore_SCE_to_Default.vbs** script on the computer you wish to update.
3. Follow the onscreen prompts.

# Additional Security Settings

Although most of the countermeasures that were used to harden the client systems in the two environments that are discussed in this chapter were applied through Group Policy, there are additional settings that are difficult or impossible to apply with Group Policy. For a detailed explanation of each of the countermeasures discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

## *Manual Hardening Procedures*

This section describes how some additional countermeasures were implemented manually to secure the Windows XP clients for each of the security environments that are defined in this guide.

## Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger

Some organizations may feel that system debuggers such as the Dr. Watson tool that is included with Windows could be exploited by knowledgeable attackers. For instructions about how to disable the Dr. Watson system debugger, see the Microsoft Knowledge Base article "How to disable Dr. Watson for Windows," which is available online at http://support.microsoft.com/default.aspx?scid=188296.

## Disable SSDP/UPNP: Disable SSDP/UPNP

Some organizations may feel that the Universal Plug and Play features that are included with subcomponents of Windows XP should be completely disabled. Although the **Universal Plug and Play host** service is disabled in this guide, other applications such as Windows Messenger will use the **Simple Service Discovery Protocol (SSDP) discovery service** process to identify network gateways or other network devices. You can ensure that no applications use the SSDP and UPnP features that are included with Windows XP by adding a REG_DWORD registry value called **UPnPMode** to the **HKEY_LOCAL_MACHINE\Software\Microsoft\DirectPlayNATHelp\DPNHUPnP** registry key and setting its value to **2**.

For more information, see the Microsoft Knowledge Base article "Traffic Is Sent After You Turn Off the SSDP Discover Service and Universal Plug and Play Device Host," which is available online at http://support.microsoft.com/default.aspx?scid=317843.

# Securing the File System

The NTFS file system has been improved with each new version of Microsoft Windows. The default permissions for NTFS are adequate for most organizations. The settings that are discussed in this section are for organizations that use laptops and desktops in the Specialized Security – Limited Functionality (SSLF) environment that is defined in this guide.

File system security settings may be modified through Group Policy. You can configure the file system settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Windows Settings\Security Settings\File System**

**Note**: Any changes to the default file system security settings should be thoroughly tested in a lab environment before they are deployed in a large organization. There have been cases in which file permissions have been altered to a point that required the affected computers to be completely rebuilt.

The default file permissions in Windows XP are sufficient for most situations. However, if you are not going to block membership of the **Power Users** group with the Restricted Groups feature or if you are going to enable the **Network access: Let Everyone permissions apply to anonymous users** setting, you may want to apply the optional permissions that are described in the next paragraph. These optional permissions are very specific, and they apply additional restrictions to certain executable tools that a malicious user with elevated privileges may use to further compromise the system or network.

Note that these permission changes do not affect multiple folders or the root of the system volume. It can be very risky to change permissions in that manner, and doing so can often cause system instability. All of the files are located in the **%SystemRoot%\System32** folder, and they are all given the following permissions: **Administrators: Full Control, System: Full Control**.

- regedit.exe
- arp.exe
- at.exe
- attrib.exe
- cacls.exe
- debug.exe
- edlin.exe
- eventcreate.exe
- eventtriggers.exe
- ftp.exe
- nbtstat.exe
- net.exe
- net1.exe
- netsh.exe
- netstat.exe
- nslookup.exe
- ntbackup.exe
- rcp.exe
- reg.exe
- regedt32.exe
- regini.exe
- regsvr32.exe
- rexec.exe
- route.exe
- rsh.exe
- sc.exe
- secedit.exe
- subst.exe
- systeminfo.exe
- telnet.exe
- tftp.exe
- tlntsvr.exe

For your convenience, these optional permissions are already configured in the security template called Optional-File-Permissions.inf, which is included with the downloadable version of this guide.

# *Advanced Permissions*

You can set file permissions with more control than they initially appear to offer in the **Permissions** dialog box. To do so, click the **Advanced** button. The following table describes these advanced permissions.

**Table 3.22 Advanced File Permissions and Descriptions**

| Advanced permission name | Description |
|---|---|
| Traverse Folder/Execute | Allows or denies user requests to move through folders to reach other files or folders, even if the user has no permission to traverse folders (applies to folders only). |
| List Folders/Read Data | Allows or denies user requests to view file names and subfolder names within the specified folder. It only affects the contents of that folder and does not affect whether the folder on which you are setting the permission will be listed (applies to folders only). |
| Read Attributes | Allows or denies the ability to view data in files (applies to files only). |
| Read Extended Attributes | Allows or denies user requests to view the attributes of a file or folder, such as read-only and hidden. Attributes are defined by NTFS. |

| Advanced permission name | Description |
|---|---|
| Create Files/Write Data | Create Files allows or denies creating files within the folder (applies to folders only). Write Data allows or denies the ability to make changes to the file and overwrite existing content (applies to files only). |
| Create Folders/Append Data | Create Folders allows or denies user requests to create folders within a specified folder (applies to folders only). Append Data allows or denies the ability to make changes to the end of the file but not to change, delete, or overwrite existing data (applies to files only). |
| Write Attributes | Allows or denies user requests to make changes to the end of the file, but not to change, delete, or overwrite existing data (applies to files only). |
| Write Extended Attributes | Allows or denies user requests to change the attributes of a file or folder, such as read-only or hidden. Attributes are defined by NTFS. |
| Delete Subfolders and Files | Allows or denies the ability to delete subfolders and files, even if the Delete permission has not been assigned on the subfolder or file (applies to folders). |
| Delete | Allows or denies user requests to delete subfolders and files, even if the Delete permission has not been assigned on the subfolder or file (applies to folders). |
| Read Permissions | Allows or denies user requests to read the permissions of files or folders, such as Full Control, Read, and Write. |
| Change Permissions | Allows or denies user requests to change permissions of files or folders, such as Full Control, Read, and Write. |
| Take Ownership | Allows or denies taking ownership of the file or folder. The owner of a file or folder can always change permissions on it, regardless of any existing permissions that protect the file or folder. |

The following three additional terms are used to describe the inheritance of permissions that are applied to files and folders:

- **Propagate** refers to the propagation of inheritable permissions to all subfolders and files. Any child objects of an object inherit the parent object's security settings, provided the child object is not protected from accepting permission inheritance. If there is a conflict, the explicit permissions on the child object will override the permissions that are inherited from the parent object.
- **Replace** refers to the replacement of existing permissions on all subfolders and files with inheritable permissions. The parent object's permission entries will override any security settings on the child object, regardless of the child object's settings. The child object will have identical access control entries as the parent object.
- **Ignore** refers to not allowing permissions on a file or folder (or key) to be replaced. Use this configuration option if you do not want to configure or analyze security for this object or any of its child objects.

# Summary

This chapter described in detail the primary security settings and recommended configurations for each setting to secure computers that run Windows XP Professional with SP2 in the two environments that are discussed in this chapter. When you consider the security policies for your organization, remember the trade-offs between security and user productivity. Although users need protection from malicious code and attackers, they also need to perform their jobs without overly restrictive security policies that frustrate their efforts.

# *More Information*

The following links provide additional information about Windows XP Professional security-related topics.

- For more information about how to maintain security for Windows XP Professional, see the Help and Support tool that is included with Windows XP and the Microsoft Windows XP Security and Privacy Web site at http://www.microsoft.com/windowsxp/using/security/default.mspx.
- For more information about the security features in Windows XP SP2, see "Security Information for Windows XP Service Pack 2" at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpsp2sec.mspx.
- For more information about security settings available in Windows XP SP2, see the Microsoft TechNet article "Security Setting Descriptions" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/dd980ca3-f686-4ffc-a617-50c6240f5582.mspx.
- For more information about secure channels, see the Windows 2000 Magazine article "Secure Channels in NT 4.0" at http://msdn.microsoft.com/archive/en-us/dnarntmag00/html/secure.asp.
- For more information about security for the Windows operating system, see the Microsoft Windows Security Resource Kit at http://www.microsoft.com/MSPress/books/6418.asp.
- For more information about the Encrypting File System feature of Windows XP and Windows Server 2003, see "Encrypting File System in Windows XP and Windows Server 2003" at http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx.

# Chapter 4: Administrative Templates for Windows XP

## Overview

This chapter describes in detail how to configure and apply additional security settings to Microsoft® Windows® XP Professional with Service Pack 2 (SP2) by using Administrative Templates. Administrative Template (.adm) files are used to configure settings in the Windows XP registry that govern the behavior of many services, applications, and operating system components.

Five of the Administrative Templates that ship with Windows XP SP2 include hundreds of additional settings that you can use to improve the security of Windows XP Professional. There are several settings in the Microsoft Windows Server™ 2003 Administrative Templates that do not work with Windows XP. For a complete listing of all the Administrative Template settings that are available with Windows XP, see the Microsoft Excel® workbook "Policy Settings" that is referenced in the “More Information” section at the end of this chapter.

The following table lists the .adm files and the applications and services that they affect.

**Table 4.1 Administrative Template Files**

| File name | Operating system | Description |
|---|---|---|
| System.adm | Windows XP Professional | Contains many settings to customize the user’s operating environment. |
| Inetres.adm | Windows XP Professional | Contains settings for Internet Explorer 6.0. |
| Conf.adm | Windows XP Professional | Contains settings to configure Microsoft NetMeeting®. |
| Wmplayer.adm | Windows XP Professional | Contains settings to configure Windows Media Player. |
| Wuau.adm | Windows XP Professional | Contains settings to configure Windows Update. |

**Note**: You must manually configure the Administrative Template settings in the Group Policy object (GPO) to apply them to the computers and users in your environment.

There are two major groups of settings in the Administrative Templates:

- Computer Configuration settings (stored in the **HKEY_Local_Machine** registry hive)
- User Configuration settings (stored in the **HKEY_Current_User** registry hive)

As in Chapter 3, "Security Settings for Windows XP Clients," setting prescriptions are included for the Enterprise Client (EC) and Specialized Security – Limited Functionality (SSLF) environments that are defined in this guide.

**Note**: The user settings are applied to an organizational unit (OU) that contains users through a linked GPO. See Chapter 2, "Configuring the Active Directory Domain Infrastructure," for additional details about this OU.

Some settings are available under both Computer Configuration and User Configuration in the Group Policy Object Editor. If a setting that applies to a user who logs on to a computer that has had the same Computer Configuration setting applied to it through Group Policy, the Computer Configuration setting takes precedence over the User Configuration setting.

Previous versions of this guide contained information about settings for Office XP. However, these settings have now been updated for Office 2003 and are available on the Microsoft Web site. See the "More Information" section at the end of this chapter for links to this information.

This chapter does not describe all possible settings that are available in the Administrative Templates provided by Microsoft; many of these settings are user interface (UI) settings that are not specific to security. Decisions about which of the prescribed setting configurations in this guidance apply to your environment should be based on the security goals of your organization.

If there are additional settings you want to apply through Group Policy to Windows XP Professional, you can develop your own custom templates. See the white papers listed in the “More Information” section at the end of this chapter for detailed information about how to develop your own Administrative Templates.

# Computer Configuration Settings

The following sections discuss the settings that are prescribed under Computer Configuration in the Group Policy Object Editor. Configure these settings at the following location:

**Computer Configuration\Administrative Templates**

This location is shown in context in the following figure:

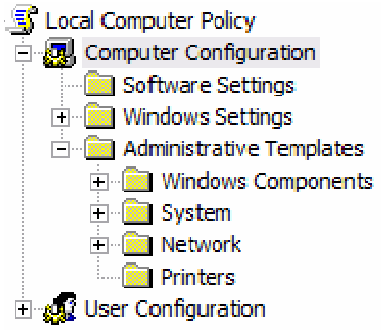


**Figure 4.1 Group Policy structure for Computer Configuration**

The structure of this chapter is based on the container structure in Group Policy. Tables in the following sections summarize setting recommendations for various Computer Configuration options, and recommendations are provided for both desktop and laptop client computers in two types of secure environments—the Enterprise Client (EC) environment and the Specialized Security – Limited Functionality (SSLF) environment. More detailed information about each of the settings is provided in the subsections that follow each table.

Apply these settings through a GPO that is linked to an OU that contains the computer accounts in your environment. Include the laptop settings in the GPO that is linked to the laptop OU, and the desktop settings in the GPO that is linked to the desktop OU.

# Windows Components

The following figure illustrates the sections in Group Policy that will be affected by the setting changes in this section:

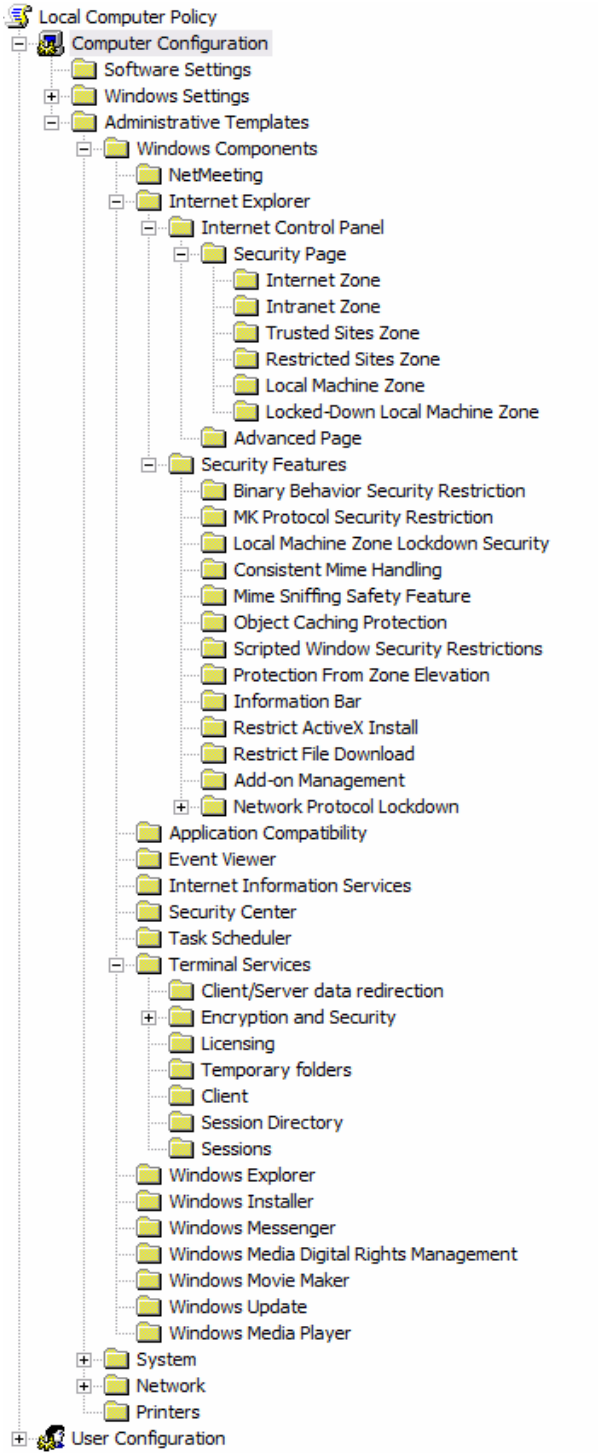


**Figure 4.2 Group Policy structure for Computer Configuration Windows Components**

# NetMeeting

Microsoft NetMeeting allows users to conduct virtual meetings across the network in your organization. You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\ NetMeeting**

**Table 4.2 Recommended NetMeeting Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Disable remote Desktop Sharing | Not Configured | Not Configured | Enabled | Enabled |

## *Disable remote Desktop Sharing*

This policy setting disables the remote desktop sharing feature of NetMeeting. If you enable this policy setting, users will not be able to configure NetMeeting to allow remote control of the local desktop.

The **Disable remote Desktop Sharing** setting is **Not Configured** for the EC environment. However, it is configured to **Enabled** for the SSLF environment to prevent users from sharing desktops remotely through NetMeeting.

# Internet Explorer

Microsoft Internet Explorer Group Policies help you enforce security requirements for Windows XP workstations, and prevent the exchange of unwanted content through Internet Explorer. Use the following criteria to secure Internet Explorer on the workstations in your environment:

- Ensure that requests to the Internet only occur in direct response to user actions.
- Ensure that information sent to specific Web sites only reaches those sites unless specific user actions are allowed to transmit information to other destinations.
- Ensure that trusted channels to servers/sites are clearly identified along with who owns the servers/sites on each channel.
- Ensure that any script or program that runs with Internet Explorer executes in a restricted environment. Programs that are delivered through trusted channels may be enabled to operate outside of the restricted environment.

You can configure the following prescribed computer settings for Internet Explorer in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

The following table summarizes many of the Internet Explorer setting recommendations. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.3 Recommended Internet Explorer Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Disable Automatic Install of Internet Explorer components | Enabled | Enabled | Enabled | Enabled |
| Disable Periodic Check for Internet Explorer software updates | Enabled | Enabled | Enabled | Enabled |
| Disable software update shell notifications on program launch | Enabled | Enabled | Enabled | Enabled |
| Do not allow users to enable or disable add-ons | Enabled | Enabled | Enabled | Enabled |
| Make proxy settings per-machine (rather than per-user) | Enabled | Disabled | Enabled | Disabled |
| Security Zones: Do not allow users to add/delete sites | Enabled | Enabled | Enabled | Enabled |
| Security Zones: Do not allow users to change policies | Enabled | Enabled | Enabled | Enabled |
| Security Zones: Use only machine settings | Enabled | Enabled | Enabled | Enabled |
| Turn off Crash Detection | Enabled | Enabled | Enabled | Enabled |

### *Disable Automatic Install of Internet Explorer components*

If you enable this policy setting, Internet Explorer will not be able to download components when users browse to Web sites that require the components to fully function. If this policy setting is disabled or not configured, users will be prompted to download and install components each time they visit Web sites that use them.

The **Disable Automatic Install of Internet Explorer components** setting is configured to **Enabled** for the two environments that are discussed in the chapter.

**Note**: Before you enable this policy setting, Microsoft recommends that you set up an alternative strategy to update Internet Explorer through Microsoft Update or a similar service.

### *Disable Periodic Check for Internet Explorer software updates*

If you enable this policy setting, Internet Explorer will not be able to determine whether a later browser version is available and notify users if this is the case. If this policy setting is disabled or not configured, Internet Explorer will check for updates every 30 days (its default setting) and notify users if a new version is available.

The **Disable Periodic Check for Internet Explorer software updates** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

**Note**: Before you enable this policy setting, Microsoft recommends that you set up an alternative strategy for the administrators in your organization to ensure that they periodically accept new updates for Internet Explorer on the client computers in your environment.

### *Disable software update shell notifications on program launch*

This policy setting specifies that programs that use Microsoft software distribution channels will not notify users when they install new components. Software distribution channels are used to update software dynamically on users' computers; this functionality is based on Open Software Distribution (.osd) technologies.

The **Disable software update shell notifications on program launch** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Do not allow users to enable or disable add-ons*

This policy setting allows you to manage whether users have the ability to allow or deny add-ons through Manage Add-ons. If you configure this policy setting to **Enabled**, users cannot enable or disable add-ons through Manage Add-ons. The only exception is if an add-on has been specifically entered into the **Add-On List** policy setting in a way that allows users to continue to manage the add-on. In such a case, the user can still manage the add-on through Manage Add-ons. If you configure this policy setting to **Disabled**, the user will be able to enable or disable add-ons.

**Note**: For more information about how to manage Internet Explorer add-ons in Windows XP with SP2, see KB article 883256, "How to manage Internet Explorer add-ons in Windows XP Service Pack 2" at http://support.microsoft.com/?kbid=883256.

Users often choose to install add-ons that are not permitted by an organization's security policy. Such add-ons can pose a significant security and privacy risk to your network. Therefore, this policy setting is configured to **Enabled** for the two environments that are discussed in this guide.

**Note**: You should review the GPO settings in Internet Explorer\Security Features\Add-on Management to ensure that appropriate authorized add-ons can still run in your environment. For example, you may want to read the Microsoft Knowledge base article "Outlook Web Access and Small Business Server Remote Web Workplace do not function if XP Service Pack 2 Add-on Blocking is enabled via group policy" at http://support.microsoft.com/default.aspx?kbid=555235.

### *Make proxy settings per-machine (rather than per-user)*

If you enable this policy setting, users will not be allowed to alter user-specific proxy settings. They must use the zones that are created for all users of the computers they access.

The **Make proxy settings per-machine (rather than per-user)** setting is configured to **Enabled** for desktop client computers for the two environments that are discussed in this chapter. However, the policy setting is configured to **Disabled** for laptop client computers because mobile users may have to change their proxy settings as they travel.

### *Security Zones: Do not allow users to add/delete sites*

Enable this policy setting to disable the site management settings for security zones. (To see the site management settings for security zones, open Internet Explorer, select **Tools** and then **Internet Options**, click the **Security** tab, and then click **Sites**.) If this policy setting is disabled or not configured, users will be able to add or remove Web sites in the **Trusted Sites** and **Restricted Sites** zones, as well as alter settings in the **Local Intranet** zone.

The **Security Zones: Do not allow users to add/delete sites** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

**Note**: If you enable the **Disable the Security page** setting (located in \User Configuration\ Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), the **Security** tab is removed from the interface and the **Disable** setting takes precedence over this **Security Zones:** setting.

### *Security Zones: Do not allow users to change policies*

If you enable this policy setting, you disable the **Custom Level** button and **Security level for this zone** slider on the **Security** tab in the **Internet Options** dialog box. If this policy setting is disabled or not configured, users will be able to change the settings for security zones. It prevents users from changing security zone policy settings that are established by the administrator.

The **Security Zones: Do not allow users to change policies** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

**Note**: If you enable the **Disable the Security page** setting (located in \User Configuration\ Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) the **Security** tab is removed from Internet Explorer in Control Panel and the **Disable** setting takes precedence over this **Security Zones:** setting.

### *Security Zones: Use only machine settings*

This policy setting affects how security zone changes apply to different users. It is intended to ensure that security zone settings remain uniformly in effect on the same computer and do not vary from user to user. If you enable this policy setting, changes that one user makes to a security zone will apply to all users of that computer. If this policy setting is disabled or not configured, users of the same computer are allowed to establish their own security zone settings.

The **Security Zones: Use only machine settings** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Turn off Crash Detection*

This policy setting allows you to manage the crash detection feature of add-on management in Internet Explorer. If you enable this policy setting, a crash in Internet Explorer will be similar to one on a computer that runs Windows XP Professional with Service Pack 1 (SP1) or earlier: Windows Error Reporting will be invoked. If you disable this policy setting, the crash detection feature in add-on management will be functional.

Because Internet Explorer crash report information could contain sensitive information from the computer's memory, the **Turn off Crash Detection** setting is configured to **Enabled** for both of the two environments that are discussed in this chapter. If you experience frequent repeated crashes and need to report them for follow-up troubleshooting, you could temporarily configure the policy setting to **Disabled**.

## Internet Explorer\Internet Control Panel\Security Page

You can configure these computer settings in the following location within the Group Policy Object Editor:

> **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page**

SP2 introduced several new policy settings to help you secure Internet Explorer zone configuration across your environment. The default values for these settings provide enhanced security compared to earlier versions of Windows. However, you might want to review these settings to determine whether you want to require them or relax them in your environment for usability or application compatibility.

For example, SP2 configures Internet Explorer to block pop-ups for all Internet zones by default. You might want to ensure that this policy setting is enforced on all computers in your environment to eliminate pop-up windows and to reduce the possibility of malicious software and spyware installations that are often spawned from Internet Web sites. Conversely, your environment might contain applications that require the use of pop-ups to function. If so, you could configure this policy to allow pop-ups for Web sites within your intranet.

# Internet Explorer\Internet Control Panel\Advanced Page

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page**

**Table 4.4 Recommended Allow Software to Run Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Allow software to run or install even if the signature is invalid | Disabled | Disabled | Disabled | Disabled |

## *Allow software to run or install even if the signature is invalid*

Microsoft ActiveX® controls and file downloads often have digital signatures attached that certify the file's integrity and the identity of the signer (creator) of the software. Such signatures help ensure that unmodified software is downloaded and that you can positively identify the signer to determine whether you trust them enough to run their software.

The **Allow software to run or install even if the signature is invalid** setting allows you to manage whether downloaded software can be installed or run by users even though the signature is invalid. An invalid signature might indicate that someone has tampered with the file. If you enable this policy setting, users will be prompted to install or run files with an invalid signature. If you disable this policy setting, users cannot run or install files with an invalid signature.

Because unsigned software can create a security vulnerability, this policy setting is configured to **Disabled** for both of the environments that are discussed in this chapter.

**Note**: Some legitimate software and controls may have an invalid signature and still be OK. You should carefully test such software in isolation before you allow it to be used on your organization's network.

# Internet Explorer\Security Features\MK Protocol Security Restriction

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\MK Protocol Security Restriction**

**Table 4.5 Recommended MK Protocol Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (MK Protocol) | Enabled | Enabled | Enabled | Enabled |

## *Internet Explorer Processes (MK Protocol)*

This policy setting reduces attack surface area because it blocks the seldom-used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. If you configure this policy setting to **Enabled**, the MK protocol is blocked for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. If you disable this policy setting, other applications are allowed to use the MK protocol API.

Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This policy setting is configured to **Enabled** for both of the environments that are discussed in this chapter. Microsoft recommends that you block the MK protocol unless you specifically need it in your environment.

**Note**: Because resources that use the MK protocol will fail when you deploy this policy setting, you should ensure that none of your applications use the protocol.

# Internet Explorer\Security Features\Consistent MIME Handling

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Consistent MIME Handling**

**Table 4.6 Recommended Consistent MIME Handling Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (Consistent MIME Handling) | Enabled | Enabled | Enabled | Enabled |

## *Internet Explorer Processes (Consistent MIME Handling)*

Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files that are received through a Web server. The **Consistent MIME Handling** setting determines whether Internet Explorer requires that all file type information that is provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted.

If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data that is provided by the file.

MIME file type spoofing is a potential threat to your organization. You should ensure that these files are consistent and properly labeled to help prevent malicious file downloads that may infect your network. This policy setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: This policy setting works in conjunction with, but does not replace, the **MIME Sniffing Safety Features** settings.

# Internet Explorer\Security Features\MIME Sniffing Safety Features

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\MIME Sniffing Safety Features**

**Table 4.7 Recommended MIME Sniffing Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (MIME Sniffing) | Enabled | Enabled | Enabled | Enabled |

### *Internet Explorer Processes (MIME Sniffing)*

MIME sniffing is a process that examines the content of a MIME file to determine its context—whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to **Enabled**, MIME sniffing will never promote a file of one type to a more dangerous file type. If you disable this policy setting, MIME sniffing configures Internet Explorer processes to allow promotion of a file from one type to a more dangerous file type. For example, a text file could be promoted to an executable file, which is dangerous because any code in the supposed text file would be executed.

MIME file-type spoofing is a potential threat to your organization. Microsoft recommends that you ensure these files are consistently handled to help prevent malicious file downloads that may infect your network.

The **Internet Explorer Processes (MIME Sniffing)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: This policy setting works in conjunction with, but does not replace, the **Consistent MIME Handling** settings.

## Internet Explorer\Security Features\Scripted Window Security Restrictions

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

> **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Scripted Window Security Restrictions**

**Table 4.8 Recommended Scripted Window Restrictions Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (Scripted Window Security Restrictions) | Enabled | Enabled | Enabled | Enabled |

### *Internet Explorer Processes (Scripted Window Security Restrictions)*

Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code.

The **Internet Explorer Processes (Scripted Window Security Restrictions)** setting restricts pop-up windows and does not allow scripts to display windows in which the title and status bars are not visible to the user or that hide other windows' title and status bars. If you enable this policy setting, pop-up windows will not display in Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts will still be able to create pop-up windows and windows that hide other windows.

The **Internet Explorer Processes (Scripted Window Security Restrictions)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter. When enabled, this policy setting makes it difficult for malicious Web sites to control your Internet Explorer windows or fool users into clicking on the wrong window.

# Internet Explorer\Security Features\Protection From Zone Elevation

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Protection From Zone Elevation**

**Table 4.9 Recommended Zone Elevation Protection Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (Zone Elevation Protection) | Enabled | Enabled | Enabled | Enabled |

## *Internet Explorer Processes (Zone Elevation Protection)*

Internet Explorer places restrictions on each Web page that it opens. These restrictions are dependent upon the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, which makes the Local Machine security zone a prime target for malicious attackers.

If you enable the **Internet Explorer Processes (Zone Elevation Protection)** setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach prevents content that runs in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes.

Because of the severity and relative frequency of zone elevation attacks, the **Internet Explorer Processes (Zone Elevation Protection)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

# Internet Explorer\Security Features\Restrict ActiveX Install

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Restrict ActiveX Install**

**Table 4.10 Restrict ActiveX Install Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (Restrict ActiveX Install) | Enabled | Enabled | Enabled | Enabled |

## *Internet Explorer Processes (Restrict ActiveX Install)*

This policy setting provides the ability to block ActiveX control installation prompts for Internet Explorer processes. If you enable this policy setting, prompts for ActiveX control installations will

be blocked for Internet Explorer processes. If you disable this policy setting, prompts for ActiveX control installations will not be blocked and these prompts will be displayed to users.

Users often choose to install software such as ActiveX controls that are not permitted by their organization's security policy. Such software can pose significant security and privacy risks to networks. Therefore, the **Internet Explorer Processes (Restrict ActiveX Install)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: This policy setting also blocks users from installing authorized legitimate ActiveX controls that will interfere with important system components like Windows Update. If you enable this policy setting, make sure to implement some alternate way to deploy security updates such as Windows Server Update Services (WSUS).

For more information about WSUS, see the Windows Server Update Services Product Overview page at http://www.microsoft.com/windowsserversystem/updateservices/evaluation/overview.mspx.

# Internet Explorer\Security Features\Restrict File Download

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Restrict File Download**

**Table 4.11 Recommended Restrict File Download Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Internet Explorer Processes (Restrict File Download) | Enabled | Enabled | Enabled | Enabled |

## *Internet Explorer Processes (Restrict File Download)*

In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download.

If you configure the **Internet Explorer Processes (Restrict File Download)** setting to **Enabled**, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting to **Disabled**, file download prompts will occur that are not user-initiated for Internet Explorer processes.

The **Internet Explorer Processes (Restrict File Download)** setting is configured to **Enabled** for both of the environments that are discussed in this chapter to help prevent attackers from placing arbitrary code on users' computers.

# Internet Explorer\Security Features\Add-on Management

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Add-on Management**

**Table 4.12 Add-on Management Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Deny all add-ons unless specifically allowed in the Add-on List | Recommended | Recommended | Recommended | Recommended |
| Add-on List | Recommended | Recommended | Recommended | Recommended |

### *Deny all add-ons unless specifically allowed in the Add-on List*

This policy setting, along with the **Add-on List** setting, allows you to control Internet Explorer add-ons. By default, the **Add-on List** setting defines a list of add-ons to be allowed or denied through Group Policy. The **Deny all add-ons unless specifically allowed in the Add-on List** setting ensures that all add-ons are assumed to be denied unless they are specifically listed in the **Add-on List** setting.

If you enable this policy setting, Internet Explorer only allows add-ins that are specifically listed (and allowed) through the **Add-on List**. If you disable this policy setting, users may use Add-on Manager to allow or deny any add-ons.

You should consider using both the **Deny all add-ons unless specifically allowed in the Add-on List** setting and the **Add-on List** setting to control the add-ons that can be used in your environment. This approach will help ensure that only authorized add-ons are used.

## *Add-on List*

This policy setting, along with the **Deny all add-ons unless specifically allowed in the Add-on List** setting, allows you to control Internet Explorer add-ons. By default, the **Add-on List** setting defines a list of add-ons to be allowed or denied through Group Policy. The **Deny all add-ons unless specifically allowed in the Add-on List** setting ensures that all add-ons are assumed to be denied unless they are specifically listed in the **Add-on List** setting.

If you enable the **Add-on List** setting, you are required to list the add-ons to be allowed or denied by Internet Explorer. The specific list of add-ons that should be included on this list will vary from one organization to another, and therefore this guide does not provide a detailed list. For each entry that you add to the list, you must provide the following information:

- **Name of the Value**. The CLSID (class identifier) for the add-on you wish to add to the list. The CLSID should be in brackets; for example, {000000000-0000-0000-0000-0000000000000}. The CLSID for an add-on can be obtained by reading the OBJECT tag from a Web page on which the add-on is referenced.
- **Value**. A number that indicates whether Internet Explorer should deny or allow the add-on to be loaded. The following values are valid:
  - **0** Deny this add-on
  - **1** Allow this add-on
  - **2** Allow this add-on and permit the user to manage it through Manage Add-ons

If you disable the **Add-on List** setting, the list is deleted. You should consider using both the **Deny all add-ons unless specifically allowed in the Add-on List** and the **Add-on List** settings to control the add-ons that can be used in your environment. This approach will help ensure that only authorized add-ons are used.

# Terminal Services\Client/Server data redirection

Terminal Services settings provide options to redirect client computer resources to servers that are accessed through Terminal Services. The following setting is specific to Terminal Services.

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client/Server data redirection**

**Table 4.13 Recommended Do Not Allow Drive Redirection Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Do not allow drive redirection | Not Configured | Not Configured | Enabled | Enabled |

### *Do not allow drive redirection*

This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer or My Computer in the following format:

\\TSClient\<*driveletter*>$

If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them.

For this reason, the **Do not allow drive redirection** setting is configured to **Enabled** for the SSLF environment. However, this policy setting is **Not Configured** for the EC environment.

## Terminal Services\Encryption and Security

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security**

**Table 4.14 Recommended Terminal Services Encryption and Security Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Always prompt client for password upon connection | Not Configured | Not Configured | Enabled | Enabled |
| Set client connection encryption level | High Level | High Level | High Level | High Level |

### *Always prompt client for password upon connection*

This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.

The **Always prompt client for password upon connection** setting is configured to **Enabled** in the SSLF environment. However, this policy setting is **Not Configured** for the EC environment.

**Note**: If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent.

### *Set client connection encryption level*

This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session.

The encryption level is set to **High Level** to enforce 128-bit encryption for the two environments that are discussed in this chapter.

## Terminal Services\Client

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Administrative Templates\Windows Components\Terminal Services\Client**

**Table 4.15 Recommended Do Not Allow Passwords to be Saved Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Do not allow passwords to be saved | Enabled | Enabled | Enabled | Enabled |

### *Do not allow passwords to be saved*

This policy setting prevents passwords from being saved on a computer by Terminal Services clients. If you enable this policy setting, the password saving checkbox is disabled for Terminal Services clients and users will not be able to save passwords.

Because saved passwords can cause additional compromise, the **Do not allow passwords to be saved** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: If this policy setting was previously configured as **Disabled** or **Not Configured**, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server.

## Windows Messenger

Windows Messenger is used to send instant messages to other users on a computer network. The messages may include files and other attachments.

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Windows Messenger**

**Table 4.16 Recommended Windows Messenger Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Do not allow Windows Messenger to be run | Enabled | Enabled | Enabled | Enabled |

### *Do not allow Windows Messenger to be run*

You can enable the **Do not allow Windows Messenger to be run** setting to disable Windows Messenger and prevent the program from being executed. Because this application has been used for malicious purposes such as spam, the distribution of malicious software, and disclosure of sensitive data, Microsoft recommends that you configure the **Do not allow Windows Messenger to be run** setting to **Enabled** for both the EC and SSLF environments.

**Note**: If you configure this policy setting to **Enabled,** Remote Assistance is prevented from using Windows Messenger and users are prevented from using MSN® Messenger.

## Windows Update

Administrators use Windows Update settings to manage how patches and hotfixes are applied on Windows XP workstations. Updates are available from the Microsoft Windows Update Web site. Alternatively, you can set up an intranet Web site to distribute patches and hotfixes in a similar manner with additional administrative control. The Windows Update Administrative Template (WUAU.adm) was introduced with Windows XP Service Pack 1 (SP1).

Windows Server Update Services (WSUS) is an infrastructure service that builds on the success of the Microsoft Windows Update and Software Update Services (SUS) technologies. WSUS manages and distributes critical Windows patches that resolve known security vulnerabilities and other stability issues with Microsoft Windows operating systems.

WSUS eliminates manual update steps with a dynamic notification system for critical updates that are available to Windows client computers through your intranet server. No Internet access is required from client computers to use this service. This technology also provides a simple and automatic way to distribute updates to your Windows workstations and servers.

Windows Server Update Services also offers the following features:

- **Administrator control over content synchronization within your intranet**. This synchronization service is a server-side component that retrieves the latest critical updates from Windows Update. As new updates are added to Windows Update, the server running WSUS automatically downloads and stores them, based on an administrator-defined schedule.
- **An intranet-hosted Windows Update server**. This easy-to-use server acts as the virtual Windows Update server for client computers. It contains a synchronization service and administrative tools for managing updates. It services requests for approved updates from client computers that are connected to it through the HTTP protocol. This server can also host critical updates that are downloaded from the synchronization service and refer client computers to those updates.
- **Administrator control over updates**. The administrator can test and approve updates from the public Windows Update site before deployment on their organization's intranet. Deployment takes place on a schedule that the administrator creates. If multiple servers are running WSUS, the administrator controls which computers access particular servers that run the service. Administrators can enable this level of control with Group Policy in an Active Directory® directory service environment or through registry keys.
- **Automatic updates on computers (workstations or servers)**. Automatic Updates is a Windows feature that can be set up to automatically check for updates that are published on Windows Update. WSUS uses this Windows feature to publish administrator approved updates on an intranet.

**Note**: If you choose to distribute patches through another method, such as Microsoft Systems Management Server, this guide recommends that you disable the **Configure Automatic Updates** setting.

There are several Windows Update settings. A minimum of three settings is required to make Windows Update work: **Configure Automatic Updates**, **No auto-restart for scheduled Automatic Updates installations**, and **Reschedule Automatic Updates scheduled**

**installations**. A fourth setting is optional and depends on the requirements of your organization: **Specify intranet Microsoft update service location**.

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Windows Update**

The settings that are discussed in this section do not individually address specific security risks, but relate more to administrator preference. However, configuration of Windows Update is essential to the security of your environment because it ensures that the client computers in your environment receive security patches from Microsoft soon after they are available.

**Note**: Windows Update is dependent on several services, including the Remote Registry service and the Background Intelligence Transfer Service. In Chapter 3, "Security Settings for Windows XP Clients," these services are disabled in the SSLF environment. Therefore, if these services are disabled, Windows Update will not work, and the following four setting prescriptions may be disregarded for the SSLF environment only.

The following table summarizes the recommended Windows Update settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.17 Recommended Windows Update Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box | Disabled | Disabled | Disabled | Disabled |
| Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box | Disabled | Disabled | Disabled | Disabled |
| Configure Automatic Updates | Enabled | Enabled | Enabled | Enabled |
| No auto-restart for scheduled Automatic Updates installations | Disabled | Disabled | Disabled | Disabled |
| Reschedule Automatic Updates scheduled installations | Enabled | Enabled | Enabled | Enabled |
| Specify intranet Microsoft update service location | Enabled | Enabled | Enabled | Enabled |

## *Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box*

This policy setting allows you to manage whether the **Install Updates and Shut Down** option is displayed in the **Shut Down Windows** dialog box. If you disable this policy setting, the **Install Updates and Shut Down** option will display in the **Shut Down Windows** dialog box if updates are available when the user selects the **Shut Down** option in the **Start** menu or clicks **Shut Down** after pressing CTRL+ALT+DELETE.

Because updates are important to the overall security of all computers, the **Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box** setting is configured to **Disabled** for both of the environments that are discussed in this chapter. This policy setting works in conjunction with the following **Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box** setting.

### *Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box*

This policy setting allows you to manage whether the **Install Updates and Shut Down** option is allowed to be the default choice in the **Shut Down Windows** dialog. If you disable this policy setting, the **Install Updates and Shut Down** option will be the default option in the **Shut Down Windows** dialog box if updates are available for installation when the user selects the **Shut Down** option in the **Start** menu.

Because updates are important to the overall security of all computers, the **Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box** setting is configured to **Disabled** for both of the environments that are discussed in this chapter.

**Note**: This policy setting has no effect if the **Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not display 'Install Updates and Shut Down'** option in the **Shut Down Windows** dialog box setting is **Enabled**.

### *Configure Automatic Updates*

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to **Enabled**, the operating system will recognize when a network connection is available and then use the network connection to search the Windows Update Web site or your designated intranet site for updates that apply to them.

After you configure this policy setting to **Enabled**, select one of the following three options in the **Configure Automatic Updates Properties** dialog box to specify how the service will work:

- **Notify before downloading any updates and notify again before installing them**.
- **Download the updates automatically and notify when they are ready to be installed**. **(Default setting)**
- **Automatically download updates and install them on the schedule specified below**.

If you disable this policy setting, you will need to download and manually install any available updates from the Windows Update Web site at http://windowsupdate.microsoft.com.

The **Configure Automatic Updates** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *No auto-restart for scheduled Automatic Updates installations*

If this policy setting is enabled, the computer will wait for a logged-on user to restart it to complete a scheduled installation; otherwise, the computer will restart automatically. When enabled, this policy setting also prevents Automatic Updates from restarting computers automatically during a scheduled installation. If a user is logged on to a computer when Automatic Updates requires a restart to complete an update installation, the user is notified and given the option to delay the restart. Automatic Updates will not detect future updates until the restart occurs.

If the **No auto-restart for scheduled Automatic Updates installations** setting is configured to **Disabled** or **Not Configured**, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation. If automatic restarts are a concern, you can configure the **No auto-restart for scheduled Automatic Updates installations** setting to **Enabled**. If you do enable this policy setting, schedule your client computers to restart after normal business hours to ensure that the installation is completed.

The **No auto-restart for scheduled Automatic Updates installations** setting is configured to **Disabled** for the two environments that are discussed in this chapter.

**Note**: This policy setting only works when Automatic Updates is configured to perform scheduled update installations. If the **Configure Automatic Updates** setting is configured to **Disabled**, it will not work. A restart is generally required to complete an update installation.

### *Reschedule Automatic Updates scheduled installations*

This policy setting determines the amount of time before previously scheduled Automatic Update installations will proceed after system startup. If you configure this policy setting to **Enabled**, a previously scheduled installation will begin after a specified number of minutes when you next start the computer. If you configure this policy setting to **Disabled** or **Not Configured**, previously scheduled installations will occur during the next regularly scheduled installation time.

The **Reschedule Automatic Updates scheduled installations** setting is configured to **Enabled** for the two environments that are discussed in this chapter. After you enable this policy setting, you may change the default waiting period to one that is appropriate for your environment.

**Note**: This policy setting only works when Automatic Updates is configured to perform scheduled update installations. If the **Configure Automatic Updates** setting is **Disabled**, the **Reschedule Automatic Updates scheduled installations** setting has no effect. You can enable the latter two settings to ensure that previously missed installations will be scheduled to install each time the computer restarts.

### *Specify intranet Microsoft update service location*

This policy setting specifies an intranet server to host updates that are available from the Microsoft Update Web sites. You can then use this update service to automatically update computers on your network. This policy setting lets you specify a WSUS server on your network to function as an internal update service. The Automatic Updates client will work with the WSUS server to search the service for updates that apply to the computers on your network.

The **Specify intranet Microsoft update service location** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: An enabled **Specify intranet Microsoft update service location** setting has no effect if the **Configure Automatic Updates** setting is disabled.

## *System*

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\System**

The following figure illustrates the sections in Group Policy that will be affected by the setting changes in this section:

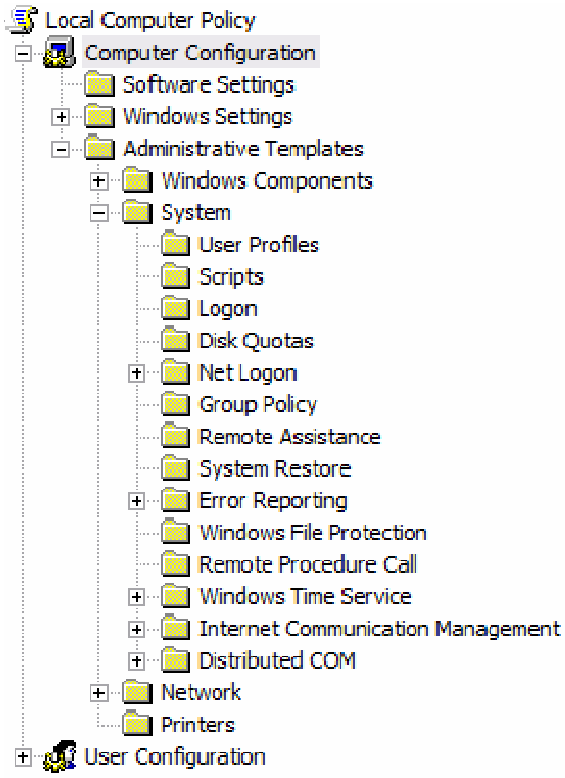


**Figure 4.3 Group Policy structure for Computer Configuration System**

The following table summarizes the recommended system settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.18 Recommended System Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Turn off Autoplay | Not Configured | Not Configured | Enabled – All Drives | Enabled – All Drives |
| Turn off Windows Update device driver search prompt | Disabled | Disabled | Enabled | Enabled |

# Turn off Autoplay

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the **Turn off Autoplay** setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

The **Turn off Autoplay** setting is configured to **Enabled – All Drives** for the SSLF environment only. However, this policy setting is **Not Configured** for the EC environment.

**Note**: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives.

## Turn off Windows Update device driver search prompt

This policy setting controls whether the administrator is prompted to search Windows Update for device drivers through the Internet. If this policy setting is **Enabled**, administrators will not be prompted to search Windows Update. If both this policy setting and **Turn off Windows Update device driver searching** are **Disabled** or **Not Configured**, the administrator will be prompted for consent before Windows Update is searched for device drivers.

Because there is some risk involved when any device drivers are downloaded from the Internet, the **Turn off Windows Update device driver search prompt** setting is configured to **Enabled** for the SSLF environment and **Disabled** for the EC environment. The reason for this recommendation is because the types of attacks that can exploit a driver download will typically be mitigated by proper enterprise resource management.

**Note**: This policy setting is only effective if the **Turn off Windows Update device driver searching** setting in **Administrative Templates/System/Internet Communication Management/Internet Communication** is **Disabled** or **Not Configured**.

# Logon

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\System\Logon**

The following table summarizes the recommended Logon settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.19 Recommended Logon Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Do not process the legacy run list | Not Configured | Not Configured | Enabled | Enabled |
| Do not process the run once list | Not Configured | Not Configured | Enabled | Enabled |

### *Do not process the legacy run list*

This policy setting causes the run list, which is a list of programs that Windows XP runs automatically when it starts, to be ignored. The customized run lists for Windows XP are stored in the registry at the following locations:

- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**
- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**

You can enable the **Do not process the legacy run list** setting to prevent a malicious user from running a program each time Windows XP starts, which could compromise data on the computer or cause other harm. When this policy setting is enabled, certain system programs are prevented from running, such as antivirus software, and software distribution and monitoring software. Microsoft recommends that you evaluate the threat level to your environment before you determine whether to use this policy setting for your organization.

The **Do not process the legacy run list** setting is **Not Configured** for the EC environment and **Enabled** for the SSLF environment.

### *Do not process the run once list*

This policy setting causes the run-once list, which is the list of programs that Windows XP runs automatically when it starts, to be ignored. This policy setting differs from the **Do not process the legacy run list** setting in that programs on this list will run once the next time the client computer restarts. Setup and installation programs are sometimes added to this list to complete installations after a client computer restarts. If you enable this policy setting, attackers will not be able to use the run-once list to launch rogue applications, which was a common method of attack in the past. A malicious user can exploit the run-once list to install a program that may compromise the security of Windows XP client computers.

**Note**: Customized run-once lists are stored in the registry at the following location: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce**.

The **Do not process the run once list** setting should cause minimal functionality loss to users in your environment, especially if the client computers have been configured with all of your organization's standard software before this policy setting is applied through Group Policy.

The **Do not process the run once list** setting is set to **Not Configured** for the EC environment and to **Enabled** for the SSLF environment.

## Group Policy

You can configure the following prescribed computer setting in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\System\Group Policy**

**Table 4.20 Recommended Group Policy Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Registry policy processing | Enabled | Enabled | Enabled | Enabled |

### *Registry policy processing*

This policy setting determines when registry policies are updated. It affects all policies in the Administrative Templates folder, and any other policies that store values in the registry. If this policy setting is enabled, the following options are available:

- **Do not apply during periodic background processing.**
- **Process even if the Group Policy objects have not changed.**

Some settings that are configured through the Administrative Templates are made in areas of the registry that are accessible to users. User changes to these settings will be overwritten if this policy setting is enabled.

The **Registry policy processing** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

## Remote Assistance

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\System\Remote Assistance**

The following table summarizes the recommended Remote Assistance settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.21 Recommended Remote Assistance Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Offer Remote Assistance | Not Configured | Not Configured | Disabled | Disabled |
| Solicit Remote Assistance | Not Configured | Not Configured | Disabled | Disabled |

## *Offer Remote Assistance*

This policy setting determines whether a support person or an IT "expert" administrator can offer remote assistance to computers in your environment if a user does not explicitly request assistance first through a channel, e-mail, or Instant Messenger.

**Note**: The expert cannot connect to the computer unannounced or control it without permission from the user. When the expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the **Yes** button to allow the expert to remotely control the workstation after the **Offer Remote Assistance** setting is configured to **Enabled**.

If this policy setting is enabled the following options are available:

- **Allow helpers to only view the computer**
- **Allow helpers to remotely control the computer**

When you configure this policy setting, you can also specify a list of users or user groups known as "helpers" who may offer remote assistance.

**To configure the list of helpers**

1. In the **Offer Remote Assistance** setting configuration window, click **Show**. A new window will open in which you can enter helper names.
2. Add each user or group to the **Helper** list in one of the following formats:
   - *<Domain Name>\<User Name>*
   - *<Domain Name>\<Group Name>*

If this policy setting is disabled or not configured, users and or groups will not be able to offer unsolicited remote assistance to computer users in your environment.

The **Offer Remote Assistance** setting is **Not Configured** for the EC environment. However, this policy setting is configured to **Disabled** for the SSLF environment to prevent access to Windows XP client computers across the network.

## *Solicit Remote Assistance*

This policy setting determines whether remote assistance may be solicited from the Windows XP computers in your environment. You can enable this policy setting to allow users to solicit remote assistance from IT "expert" administrators.

**Note**: Experts cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the **Yes** button to allow the expert to remotely control the workstation.

If the **Solicit Remote Assistance** setting is enabled, the following options are available:

- **Allow helpers to remotely control the computer**
- **Allow helpers to only view the computer**

Also, the following options are available to configure the amount of time that a user help request remains valid:

- **Maximum ticket time (value):**
- **Maximum ticket time (units): hours, minutes or days**

When a ticket (help request) expires, the user must send another request before an expert can connect to the computer. If you disable the **Solicit Remote Assistance** setting, users cannot send help requests and the expert cannot connect to their computers.

If the **Solicit Remote Assistance** setting is not configured, users can configure solicited remote assistance through the Control Panel. The following settings are enabled by default in the Control Panel: **Solicited remote assistance**, **Buddy support**, and **Remote control**. The value for the **Maximum ticket time** is set to **30 days**. If this policy setting is disabled, no one will be able to access Windows XP client computers across the network.

The **Solicit Remote Assistance** setting is **Not Configured** for the EC environment and is configured to **Disabled** for the SSLF environment.

# Error Reporting

These settings control how operating system and application errors are reported. In the default configuration, when an error occurs the user is queried by a pop-up dialog box about whether they want to send an error report to Microsoft. Microsoft has strict policies in place to protect data that is received in these reports. However, the data is transmitted in plaintext, which is a potential security risk.

Microsoft provides the Corporate Error Reporting tool for organizations to collect the reports locally and not send them to Microsoft over the Internet. Microsoft recommends the use of the Corporate Error Reporting tool in the SSLF environment to prevent sensitive information from exposure on the Internet. Additional information about this tool is included in the “More Information” section at the end of this chapter.

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\System\Error Reporting**

The following table summarizes the recommended Error Reporting settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.22 Recommended Error Reporting Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Display Error Notification | Enabled | Enabled | Enabled | Enabled |
| Configure Error Reporting | Enabled | Enabled | Enabled | Enabled |

## *Display Error Notification*

This policy setting controls whether error messages are displayed to users on their computer screens. If you enable this policy setting, error message notifications will be sent when errors occur and users will have access to details about the errors. If you disable this policy setting, users are prevented from viewing error notifications.

When an error occurs, it is important that the user is aware of the problem. Users will not be made aware of problems if you disable the **Display Error Notification** setting. For this reason, the **Display Error Notification** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Configure Error Reporting*

This policy setting controls whether errors are reported. When this policy setting is enabled, users can choose whether to report errors when they occur. Errors may be reported to Microsoft through the Internet or to a local file share. If you enable this policy setting, the following options are also available:

- **Do not display links to any Microsoft-provided "more information" Web sites**
- **Do not collect additional files**
- **Do not collect additional machine data**
- **Force queue mode for application errors**
- **Corporate upload file path**
- **Replace instances of the word "Microsoft" with**

If the **Configure Error Reporting** setting is disabled, users are unable to report errors. If the **Display Error Notification** setting is enabled, users will receive error notifications but cannot report them. The **Configure Error Reporting** setting allows you to customize an error reporting strategy for your organization and collect reports for local analysis.

The **Configure Error Reporting** setting is configured to **Enabled** for the two environments that are discussed in this chapter. In addition, the following options were selected for the SSLF environment:

- **Do not collect additional files**
- **Do not collect additional machine data**
- **Force queue mode for application errors**

You can also select the **Corporate upload file path** option and include the path to the server on which you have installed the Corporate Error Reporting tool. You should evaluate the needs of your organization to determine which of these options to use.

## Remote Procedure Call

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Administrative Templates\System\Remote Procedure Call**

The following table summarizes the recommended Remote Procedure Call settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.23 Recommended Remote Procedure Call Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Restrictions for Unauthenticated RPC clients | Enabled–Authenticated | Enabled–Authenticated | Enabled–Authenticated | Enabled–Authenticated |
| RPC Endpoint Mapper Client Authentication | Disabled | Disabled | Enabled | Enabled |

### *Restrictions for Unauthenticated RPC clients*

This policy setting configures the RPC Runtime on an RPC server to restrict unauthenticated RPC clients from connecting to the RPC server. A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC interfaces that have specifically asked to be accessible by unauthenticated clients may be exempt from this

restriction, depending on the selected value for this policy. If you enable this policy setting, the following values are available:

- **None**. Allows all RPC clients to connect to RPC servers that run on the computer on which the policy is applied.
- **Authenticated**. Allows only authenticated RPC clients to connect to RPC servers that run on the computer on which the policy is applied. Interfaces that have asked to be exempt from this restriction will be granted an exemption.
- **Authenticated without exceptions**. Allows only authenticated RPC clients to connect to RPC servers that run on the computer on which the policy is applied. No exceptions are allowed.

Because unauthenticated RPC communication can create a security vulnerability, the **Restrictions for Unauthenticated RPC clients** setting is configured to **Enabled** and the **RPC Runtime Unauthenticated Client Restriction to Apply** value is set to **Authenticated** for both of the environments that are discussed in this chapter.

**Note**: RPC applications that do not authenticate unsolicited inbound connection requests may not work properly when this configuration is applied. Ensure you test applications before you deploy this policy setting throughout your environment. Although the Authenticated value for this policy setting is not completely secure, it can be useful for providing application compatibility in your environment.

### *RPC Endpoint Mapper Client Authentication*

If you enable this policy setting, client computers that communicate with this computer will be forced to provide authentication before an RPC communication is established. By default, RPC clients will not use authentication to communicate with the RPC Server Endpoint Mapper Service when they request the endpoint of a server. However, this default was changed for the SSLF environment to require client computers to authenticate before an RPC communication is allowed.

## Internet Communication Management\Internet Communication settings

There are several configuration settings available in the Internet Communication settings group. This guide recommends that many of these settings be restricted, primarily to help improve the confidentiality of the data on your computer systems. If these settings are not restricted, information could be intercepted and used by attackers. Although the actual occurrence of this type of attack today is rare, proper configuration of these settings will help protect your environment against future attacks.

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

> **Administrative Templates\System\Internet Communication Management\Internet Communication settings**

The following table summarizes the recommended Internet Communication settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.24 Recommended Internet Communication Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Turn off the Publish to Web task for files and folders | Enabled | Enabled | Enabled | Enabled |
| Turn off Internet download for Web publishing and online ordering wizards | Enabled | Enabled | Enabled | Enabled |

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Turn off the Windows Messenger Customer Experience Improvement Program | Enabled | Enabled | Enabled | Enabled |
| Turn off Search Companion content file updates | Enabled | Enabled | Enabled | Enabled |
| Turn off printing over HTTP | Enabled | Enabled | Enabled | Enabled |
| Turn off downloading of print drivers over HTTP | Enabled | Enabled | Enabled | Enabled |
| Turn off Windows Update device driver searching | Disabled | Disabled | Enabled | Enabled |

### *Turn off the Publish to Web task for files and folders*

This policy setting specifies whether the tasks **Publish this file to the Web**, **Publish this folder to the Web**, and **Publish the selected items to the Web** are available from File and Folder Tasks in Windows folders. The Web Publishing wizard is used to download a list of providers and allow users to publish content to the Web.

If you configure the **Turn off the Publish to Web task for files and folders** setting to **Enabled**, these options are removed from the File and Folder tasks in Windows folders. By default, the option to publish to the Web is available. Because this capability could be used to expose secured content to an unauthenticated Web client computer, this policy setting is configured to **Enabled** for both the EC and SSLF environments.

### *Turn off Internet download for Web publishing and online ordering wizards*

This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards. If this policy setting is enabled, Windows is prevented from downloading providers; only the service providers that are cached in the local registry will display.

Because the **Turn off Publish to Web task for files and folders** setting was enabled for both the EC and SSLF environments (see the previous setting), this option is not needed. However, the **Turn off Internet download for Web publishing and online ordering wizards** setting is configured to **Enabled** to minimize the attack surface of client computers and to ensure that this capability cannot be exploited in other ways.

### *Turn off the Windows Messenger Customer Experience Improvement Program*

This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. You can enable this policy setting to ensure that Windows Messenger does not collect usage information and to prevent display of the user settings that enable the collection of usage information.

In large enterprise environments it may be undesirable to have information collected from managed client computers. The **Turn off the Windows Messenger Customer Experience Improvement Program** setting is configured to **Enabled** for both of the environments that are discussed in this chapter to prevent information being collected.

### *Turn off Search Companion content file updates*

This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches. If you configure this policy setting to **Enabled**, you prevent Search Companion from downloading content updates during searches.

The **Turn off Search Companion content file updates** setting is configured to **Enabled** for both the EC and SSLF environments to help control unnecessary network communications from each managed client computer.

**Note**: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select Classic Search by clicking **Start**, **Search**, **Change Preferences**, and then **Change Internet Search Behavior**.

### *Turn off printing over HTTP*

This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet. If you enable this policy setting, the client computer will not be able to print to Internet printers over HTTP.

Information that is transmitted over HTTP through this capability is not protected and can be intercepted by malicious users. For this reason, it is not often used in enterprise environments. The **Turn off printing over HTTP** setting is configured to **Enabled** for both the EC and SSLF environments to help prevent a potential security breach from an insecure print job.

**Note**: This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.

### *Turn off downloading of print drivers over HTTP*

This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP.

The **Turn off downloading of print drivers over HTTP** setting is configured to **Enabled** to prevent print drivers from being downloaded over HTTP.

**Note**: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits drivers that are not already installed locally from being downloaded.

### *Turn off Windows Update device driver searching*

This policy setting specifies whether Windows will search Windows Update for device drivers when no local drivers for a device are present.

Because there is some risk when any device drivers are downloaded from the Internet, the **Turn off Windows Update device driver searching** setting is configured to **Enabled** for the SSLF environment and **Disabled** for the EC environment. The reason for this configuration is because the types of attacks that can exploit a driver download will typically be mitigated by proper enterprise resource and configuration management.

**Note**: See also **Turn off Windows Update device driver search prompt** in **Administrative Templates/System**, which governs whether an administrator is prompted before Windows Update is searched for device drivers if a driver is not found locally.

# Network

There are no specific security-related configurations in the Network container of Group Policy. However, there are a number of very important settings in the **Network Connections\Windows Firewall** container that the following sections will explain.

The following figure illustrates the sections in Group Policy that will be affected by the setting changes in this section:

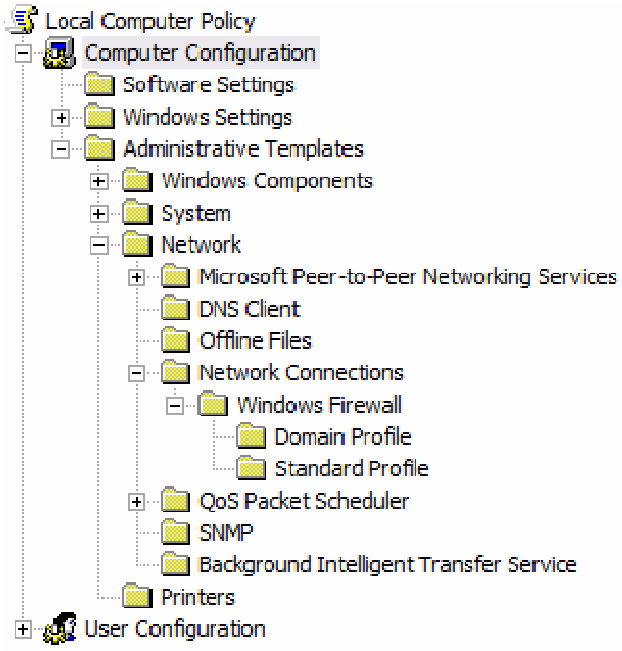


**Figure 4.4 Group Policy structure for Computer Configuration Network Connections**

# Network Connections\Windows Firewall

Windows Firewall settings are made in two profiles—Domain Profile and Standard Profile. Whenever a domain environment is detected the Domain Profile is used, and whenever a domain environment is not available the Standard Profile is used.

When a Windows Firewall setting is **Recommended** in one of the following two tables, the specific value to use will vary for different organizations. For example, each organization will have a unique list of applications that will require defined exceptions for the Windows Firewall. Therefore, it is not feasible for this guide to define a list that will be broadly useful.

When you need to determine which applications or ports may need exceptions, it may be helpful to enable Windows Firewall logging, Windows Firewall auditing, and network tracing. For more information, see the article "Configuring a Computer for Windows Firewall Troubleshooting," which is available online at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/bfdeda55-46fc-4b53-b4cd-c71838ef4b41.mspx.

For more information about how Windows XP uses Network Location Awareness (NLA) to determine what kind of network it is connected to, see the article "Network Determination Behavior for Network-Related Group Policy Settings" on the Microsoft Web site at http://www.microsoft.com/technet/community/columns/cableguy/cg0504.mspx.

Typically, the Domain Profile is configured to be less restrictive than the Standard Profile because a domain environment often provides additional layers of protection.

The policy setting names are identical in both profiles. The following two tables summarize the policy settings for the different profiles, and more detailed explanations are provided in the subsections that follow the tables.

## Network Connections\Windows Firewall\Domain Profile

The settings in this section configure the Windows Firewall Domain Profile.

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile**

**Table 4.25 Recommended Windows Firewall Domain Profile Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Protect all network Connections | Enabled | Enabled | Enabled | Enabled |
| Do not allow exceptions | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Define program exceptions | Recommended | Recommended | Recommended | Recommended |
| Allow local program exceptions | Not Recommended | Not Recommended | Disabled | Disabled |
| Allow remote administration exception | Recommended | Recommended | Disabled | Disabled |
| Allow file and printer sharing exception | Disabled | Disabled | Disabled | Disabled |
| Allow ICMP exceptions | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Allow Remote Desktop exception | Recommended | Recommended | Not Recommended | Not Recommended |
| Allow UPnP framework exception | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Prohibit notifications | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Prohibit unicast response to multicast or broadcast requests | Enabled | Enabled | Enabled | Enabled |
| Define port exceptions | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Allow local port exceptions | Disabled | Disabled | Disabled | Disabled |

**Note**: When a Windows Firewall setting is **Recommended** in this table, the specific value to use will vary for different organizations. For example, each organization will have a unique list of applications that will require defined exceptions for the Windows Firewall. Therefore, it is not feasible for this guide to define a list that will be broadly useful.

# Network Connections\Windows Firewall\Standard Profile

The settings in this section configure the Windows Firewall Standard Profile. This profile is often more restrictive than the Domain Profile, which assumes a domain environment provides some basic level of security. The Standard Profile is expected to be used when a computer is on an untrusted network, such as a hotel network or a public wireless access point. Such environments pose unknown threats and require additional security precautions.

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

**Administrative Templates\Network\Network Connections\Windows Firewall\Standard Profile**

**Table 4.26 Recommended Windows Firewall Standard Profile Settings**

| Setting | EC desktop | EC laptop | SSLF desktop | SSLF laptop |
|---|---|---|---|---|
| Protect all network Connections | Enabled | Enabled | Enabled | Enabled |
| Do not allow exceptions | Recommended | Recommended | Recommended | Recommended |
| Define program exceptions | Recommended | Recommended | Recommended | Recommended |
| Allow local program exceptions | Not Recommended | Not Recommended | Disabled | Disabled |
| Allow remote administration exception | Disabled | Disabled | Disabled | Disabled |
| Allow file and printer sharing exception | Disabled | Disabled | Disabled | Disabled |
| Allow ICMP exceptions | Disabled | Disabled | Disabled | Disabled |
| Allow Remote Desktop exception | Enabled | Enabled | Disabled | Disabled |
| Allow UPnP framework exception | Disabled | Disabled | Disabled | Disabled |
| Prohibit notifications | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Prohibit unicast response to multicast or broadcast requests | Enabled | Enabled | Enabled | Enabled |
| Define port exceptions | Not Recommended | Not Recommended | Not Recommended | Not Recommended |
| Allow local port exceptions | Disabled | Disabled | Disabled | Disabled |

**Note**: When a Windows Firewall setting is **Recommended** in this table, the specific value to use will vary for different organizations. For example, each organization will have a unique list of applications that will require defined exceptions for the Windows Firewall. Therefore, it is not feasible for this guide to define a list that will be broadly useful.

### *Windows Firewall: Protect all network connections*

This policy setting enables Windows Firewall, which replaces Internet Connection Firewall on all computers that run Windows XP with SP2. This guide recommends that you configure this policy setting to **Enabled** to protect all network connections for computers in all of the environments that are discussed in this guide.

If the **Windows Firewall: Protect all network connections** setting is configured to **Disabled**, Windows Firewall is turned off and all other settings for Windows Firewall are ignored.

**Note**: If you enable this policy setting, Windows Firewall runs and ignores the **Computer Configuration\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Firewall on your DNS domain network** setting.

### *Windows Firewall: Do not allow exceptions*

This policy setting caused Windows Firewall to block all unsolicited incoming messages. It overrides all other Windows Firewall settings that allow such messages. If you enable this policy setting in the Windows Firewall component of Control Panel, the **Don't allow exceptions** check box is selected and administrators cannot clear it.

Many environments contain applications and services that must be allowed to receive inbound unsolicited communications as part of their normal operation. Such environments may need to configure the **Windows Firewall: Do not allow exceptions** setting to **Disabled** to allow those applications and services to run properly. However, before you configure this policy setting you should test the environment to determine exactly what communications need to be allowed.

**Note**: This policy setting provides a strong defense against external attackers and should be set to **Enabled** in situations where you require complete protection from external attacks, such as the outbreak of a new network worm. If you set this policy setting to **Disabled**, Windows Firewall will be able to apply other policy settings that allow unsolicited incoming messages.

### *Windows Firewall: Define program exceptions*

Some applications may need to open and use network ports that are not typically allowed by Windows Firewall. The **Windows Firewall: Define program exceptions** setting allows you to view and change the program exceptions list that is defined by Group Policy.

If this policy setting is **Enabled** you can view and change the program exceptions list. If you add a program to this list and set its status to **Enabled**, that program can receive unsolicited incoming messages on any port that it requests Windows Firewall to open, even if that port is blocked by another setting. If you configure this policy setting to **Disabled**, the program exceptions list that is defined by Group Policy is deleted.

**Note**: If you type an invalid definition string, Windows Firewall adds it to the list without checking for errors. Because the entry is not checked, you can add programs that you have not installed yet. You can also accidentally create multiple exceptions for the same program with Scope or Status values that conflict.

### *Windows Firewall: Allow local program exceptions*

This policy setting controls whether administrators can use the Windows Firewall component in Control Panel to define a local program exceptions list. If you disable this policy setting, administrators will not be able to define a local program exceptions list; also, this configuration ensures that program exceptions only come from Group Policy. If this policy setting is enabled, local administrators are allowed to use Control Panel to define program exceptions locally.

For enterprise client computers, there may be conditions that justify local program exceptions. These conditions may include applications that were not analyzed when the organization's firewall policy was created or new applications that require nonstandard port configuration. If you choose to enable the **Windows Firewall: Allow local program exceptions** setting for such situations, remember that the attack surface of the affected computers is increased.

### *Windows Firewall: Allow remote administration exception*

Many organizations take advantage of remote computer administration in their daily operations. However, some attacks have exploited the ports that are typically used by remote administration programs; Windows Firewall can block these ports.

To provide flexibility for remote administration, the **Windows Firewall: Allow remote administration exception** setting is available. If this policy setting is enabled, the computer can receive the unsolicited incoming messages that are associated with remote administration on TCP ports 135 and 445. This policy setting also allows Svchost.exe and Lsass.exe to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034 but potentially anywhere from 1024 to 65535. If you enable this policy setting, you need to specify the IP addresses or subnets from which these incoming messages are allowed.

If you configure the **Windows Firewall: Allow remote administration exception** setting to **Disabled**, Windows Firewall makes none of the described exceptions. The impact of configuring this policy setting to **Disabled** may be unacceptable to many organizations because many remote administration tools and tools that scan for vulnerabilities will fail. Therefore, Microsoft recommends that only the most security-sensitive organizations enable this policy setting.

For the Domain Profile, Microsoft recommends that the **Windows Firewall: Allow remote administration exception** setting be **Enabled** for computers in the EC environment (if possible) and **Disabled** for computers in the SSLF environment. Computers in your environment should accept remote administration requests from as few computers as possible. To maximize the protection provided by Windows Firewall, make sure to specify only the necessary IP addresses and subnets of computers that are used for remote administration.

Microsoft recommends that the **Windows Firewall: Allow remote administration exception** setting be **Disabled** for all computers in the Standard Profile to avoid known attacks that specifically use exploits against TCP ports 135 and 445.

**Note**: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the **Windows Firewall: Allow ICMP exceptions** policy setting would block them. Policy settings that can open TCP port 445 include **Windows Firewall: Allow file and printer sharing exception**, **Windows Firewall: Allow remote administration exception**, and **Windows Firewall: Define port exceptions**.

### *Windows Firewall: Allow file and printer sharing exception*

This policy setting creates an exception that allows file and printer sharing. It configures Windows Firewall to open UDP ports 137 and 138 and TCP ports 139 and 445. If you enable this policy setting, Windows Firewall opens these ports so that the computer can receive print jobs and requests for access to shared files. You must specify the IP addresses or subnets from which such messages are allowed.

If you disable the **Windows Firewall: Allow file and printer sharing exception** setting, Windows Firewall blocks these ports and prevents the computer from sharing files and printers.

Because the computers in your environment that run Windows XP will not typically share files and printers, Microsoft recommends you configure the **Windows Firewall: Allow file and printer sharing exception** setting to **Disabled** for both of the environments that are discussed in this chapter.

**Note**: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the **Windows Firewall: Allow ICMP exceptions** policy setting would block them. Policy settings that can open TCP port 445 include **Windows Firewall: Allow file and printer sharing exception**, **Windows Firewall: Allow remote administration exception**, and **Windows Firewall: Define port exceptions**.

### *Windows Firewall: Allow ICMP exceptions*

This policy setting defines the set of Internet Control Message Protocol (ICMP) message types that Windows Firewall allows. Utilities can use ICMP messages to determine the status of other computers. For example, Ping uses the echo request message.

If you configure the **Windows Firewall: Allow ICMP exceptions** setting to **Enabled**, you must specify which ICMP message types Windows Firewall allows the computer to send or receive. When you configure this policy setting to **Disabled**, Windows Firewall blocks all unsolicited inbound ICMP message types and the listed outbound ICMP message types. As a result, utilities that rely on ICMP may fail.

Many attacker tools take advantage of computers that accept ICMP message types and use these messages to mount a variety of attacks. However, some applications require some ICMP messages in order to function properly. Also, ICMP messages are used to estimate network performance when Group Policy is downloaded and processed; if ICMP messages are blocked, Group Policy may not be applied to affected systems. For that reason, Microsoft recommends that you configure the **Windows Firewall: Allow ICMP exceptions** setting to **Disabled** whenever possible. If your environment requires some ICMP messages to get through Windows Firewall, configure this policy setting with the appropriate message types.

Whenever the computer is on an untrusted network, the **Windows Firewall: Allow ICMP exceptions** setting should be configured to **Disabled**.

**Note**: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the **Windows Firewall: Allow ICMP exceptions** policy setting would block them. Policy settings that can open TCP port 445 include **Windows Firewall: Allow file and printer sharing exception**, **Windows Firewall: Allow remote administration exception**, and **Windows Firewall: Define port exceptions**.

### *Windows Firewall: Allow Remote Desktop exception*

Many organizations use Remote Desktop connections in their normal troubleshooting procedures or operations. However, some attacks have exploited the ports that are typically used by Remote Desktop.

To provide flexibility for remote administration, the **Windows Firewall: Allow Remote Desktop** exception setting is available. If you enable this policy setting, Windows Firewall opens TCP port 3389 for inbound connections. You must also specify the IP addresses or subnets from which these inbound messages are allowed.

If you disable this policy setting, Windows Firewall blocks this port and prevents the computer from receiving Remote Desktop requests. If an administrator adds this port to a local port exceptions list in an attempt to open it, Windows Firewall does not open the port.

Some attacks can exploit an open port 3389, and therefore Microsoft recommends that you configure the **Windows Firewall: Allow Remote Desktop** setting to **Disabled** for the SSLF environment. To maintain the enhanced management capabilities that are provided by Remote Desktop, you need to configure this policy setting to **Enabled** for the EC environment. You must specify the IP addresses and subnets of the computers that are used for remote administration. Computers in your environment should accept Remote Desktop requests from as few computers as possible.

### *Windows Firewall: Allow UPnP framework exception*

This policy setting allows a computer to receive unsolicited Plug and Play messages that are sent by network devices, such as routers with built-in firewalls. To receive these messages, Windows Firewall opens TCP port 2869 and UDP port 1900.

If you enable the **Windows Firewall: Allow UPnP framework exception** setting, Windows Firewall opens these ports so that the computer can receive Plug and Play messages. You must

specify the IP addresses or subnets from which these inbound messages are allowed. If you disable this policy setting, Windows Firewall blocks these ports and prevents the computer from receiving Plug and Play messages.

Blocking UPnP network traffic effectively reduces the attack surface of computers in your environment. On trusted networks, Microsoft recommends that you configure the **Windows Firewall: Allow UPnP framework exception** setting to **Disabled** unless you use UPnP devices on your network. This policy setting should always be **Disabled** on untrusted networks.

### *Windows Firewall: Prohibit notifications*

Windows Firewall can display notifications to users when a program requests that Windows Firewall add the program to the program exceptions list. This situation occurs when programs attempt to open a port and are not allowed to do so because of current Windows Firewall rules.

The **Windows Firewall: Prohibit notifications** setting determines whether these settings are shown to the users. If you configure this policy setting to **Enabled**, Windows Firewall prevents the display of these notifications. If you configure it to **Disabled**, Windows Firewall allows the display of these notifications.

Typically, users will not be allowed to add applications and ports in response to these messages in EC or SSLF environments. In such cases, this message will inform the user of something over which they have no control and you should configure the **Windows Firewall: Prohibit notifications** setting to **Enabled**. In other environments where exceptions are allowed for some users, you should configure this policy setting to **Disabled**.

### *Windows Firewall: Prohibit unicast response to multicast or broadcast requests*

This policy setting prevents a computer from receiving unicast responses to its outgoing multicast or broadcast messages. When this policy setting is enabled and the computer sends multicast or broadcast messages to other computers, Windows Firewall blocks the unicast responses that are sent by those other computers. When this policy setting is disabled and this computer sends a multicast or broadcast message to other computers, Windows Firewall waits up to three seconds for unicast responses from the other computers and then blocks all later responses.

Typically, you would not want to receive unicast responses to multicast or broadcast messages. Such responses can indicate a denial of service (DoS) attack or an attempt to probe a known computer. Microsoft recommends that the **Windows Firewall: Prohibit unicast response to multicast or broadcast requests** setting be configured to **Enabled** to help prevent this type of attack.

**Note**: This policy setting has no effect if the unicast message is a response to a DHCP broadcast message that is sent by the computer. Windows Firewall always permits those DHCP unicast responses. However, this policy setting can interfere with the NetBIOS messages that detect name conflicts.

### *Windows Firewall: Define port exceptions*

The Windows Firewall port exceptions list should be defined by Group Policy, which allows you to centrally manage and deploy your port exceptions and ensure that local administrators do not create less secure settings.

If you enable the **Windows Firewall: Define port exceptions** setting, you can view and change the port exceptions list that is defined by Group Policy. To view and modify the port exceptions list, configure the setting to **Enabled** and then click the **Show** button. Note that if you type an invalid definition string, Windows Firewall adds it to the list without checking for errors, which means that you can accidentally create multiple entries for the same port with Scope or Status values that conflict.

If you disable the **Windows Firewall: Define port exceptions** setting, the port exceptions list that is defined by Group Policy is deleted but other settings can continue to open or block ports. Also, if a local port exceptions list exists, it is ignored unless you enable the **Windows Firewall: Allow local port exceptions** setting.

Environments with nonstandard applications that require specific ports to be open should consider program exceptions instead of port exceptions. Microsoft recommends that the **Windows Firewall: Define port exceptions** setting be configured to **Enabled** and that a list of port exceptions be specified only when program exceptions cannot be defined. Program exceptions allow the Windows Firewall to accept unsolicited network traffic only while the specified program is running, and port exceptions keep the specified ports open at all times.

**Note**: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo request messages (such as those sent by the Ping utility), even if the **Windows Firewall: Allow ICMP exceptions** policy setting would block them. Policy settings that can open TCP port 445 include **Windows Firewall: Allow file and printer sharing exception**, **Windows Firewall: Allow remote administration exception**, and **Windows Firewall: Define port exceptions**.

### *Windows Firewall: Allow local port exceptions*

This policy setting allows administrators to use the Windows Firewall component in Control Panel to define a local port exceptions list. Windows Firewall can use two port exceptions lists; the other is defined by the **Windows Firewall: Define port exceptions** setting.

If you enable the **Windows Firewall: Allow local port exceptions** setting, the Windows Firewall component in Control Panel allows administrators to define a local port exceptions list. If you disable this policy setting, the Windows Firewall component in Control Panel does not allow administrators to define such a list.

Typically, local administrators are not authorized to override organizational policy and establish their own port exceptions list in EC or SSLF security environments. For that reason, Microsoft recommends that the **Windows Firewall: Allow local port exceptions** setting be configured to **Disabled**.

# User Configuration Settings

The remaining sections of this chapter discuss User Configuration setting recommendations. Remember, these settings need to be applied to users, not computers. They should be implemented in a Group Policy that is linked to the OU that contains the users you wish to configure. You may want to refer to Figure 2.3, “Expanded OU structure to accommodate Windows XP–based desktop and laptop computers” in Chapter 2 to refresh your memory. These settings are configured in the Group Policy Object Editor at the following location:

**User Configuration\Administrative Templates**

This location is shown in context in the following figure:

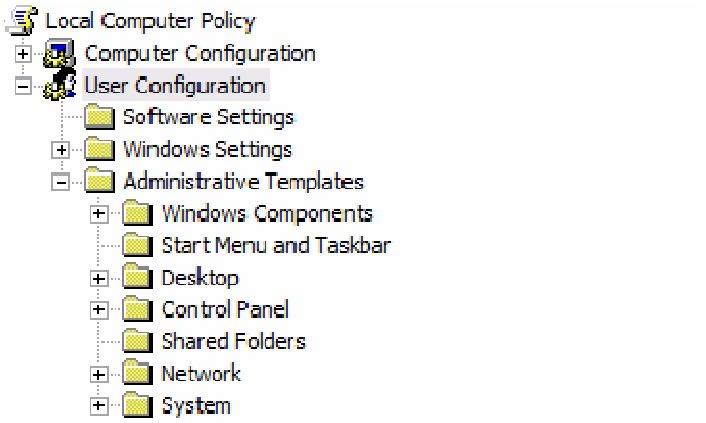


**Figure 4.5 Group Policy structure for User Configuration**

Apply these settings through a GPO that is linked to an OU that contains user accounts.

**Note**: User configuration settings are applied to any Windows XP–based computer that a user logs on to in an Active Directory domain. However, computer configuration settings apply to all client computers that are governed by a GPO in Active Directory without regard for which user logs on to the computer. For this reason, the tables in this section contain only recommended settings for the EC and the SSLF environments that are discussed in this chapter. There are no laptop or desktop prescriptions for these settings.

# Windows Components

The following figure illustrates the sections in Group Policy that will be affected by the setting changes in the Windows Components section:

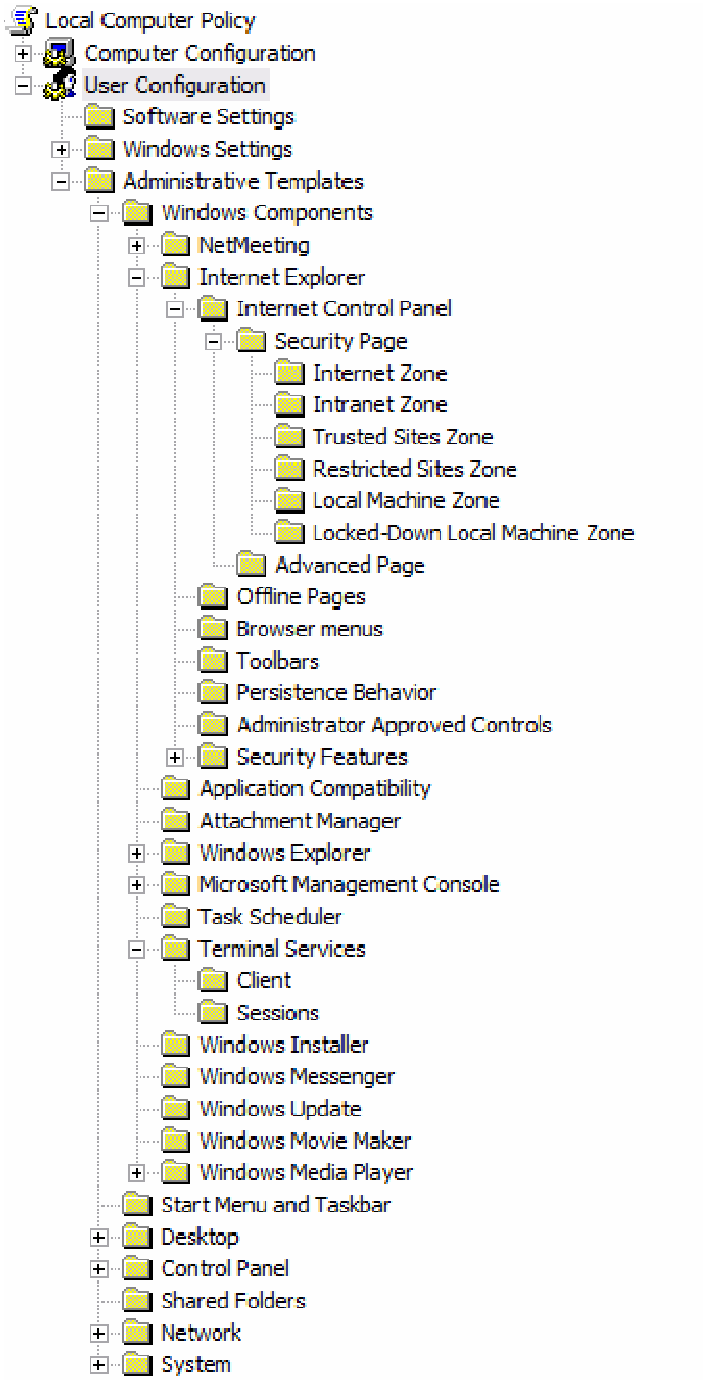


**Figure 4.6 Group Policy structure for User Configuration Windows Components**

# Internet Explorer

You can configure the following prescribed user settings in the following location within the Group Policy Object Editor:

**User Configuration\Administrative Templates\Windows Components\ Internet Explorer**

The following table summarizes the recommended Internet Explorer user configuration settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.27 Recommended Internet Explorer User Configuration Settings**

| Setting | EC computer | SSLF computer |
|---|---|---|
| Browser menus\Disable Save this program to disk option | Not Configured | Enabled |
| Internet Control Panel\Disable the Advanced Page | Not Configured | Enabled |
| Internet Control Panel\Disable the Security Page | Not Configured | Enabled |
| Offline Pages\Disable adding channels | Enabled | Enabled |
| Offline Pages\Disable adding schedules for offline pages | Enabled | Enabled |
| Offline Pages\Disable all scheduled offline pages | Enabled | Enabled |
| Offline Pages\Disable channel user interface completely | Enabled | Enabled |
| Offline Pages\Disable downloading of site subscription content | Enabled | Enabled |
| Offline Pages\Disable editing and creating of schedule groups | Enabled | Enabled |
| Offline Pages\Disable editing schedules for offline pages | Enabled | Enabled |
| Offline Pages\Disable offline page hit logging | Enabled | Enabled |
| Offline Pages\Disable removing channels | Enabled | Enabled |
| Offline Pages\Disable removing schedules for offline pages | Enabled | Enabled |
| Configure Outlook Express | Enabled | Enabled |
| Disable Changing Advanced page settings | Not Configured | Enabled |
| Disable Changing Automatic Configuration Settings | Not Configured | Enabled |
| Disable Changing Certificate Settings | Not Configured | Enabled |
| Disable Changing Connection Settings | Not Configured | Enabled |
| Disable Changing Proxy Settings | Not Configured | Enabled |
| Do not allow AutoComplete to save passwords | Enabled | Enabled |

### *Browser menus\Disable Save this program to disk option*

This policy setting prevents users from saving a program or file that Internet Explorer has downloaded to the hard disk. If you enable this policy setting, users cannot save programs to disk with the **Save This Program to Disk** option. The program file will not download, and the user is informed that the command is not available. This policy setting helps protect high security environments because users cannot download potentially harmful programs through Internet Explorer and save them to disk.

The **Browser menus\Disable Save this program to disk option** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

### *Internet Control Panel\Disable the Advanced Page*

This policy setting works in conjunction with other settings to ensure that users cannot change the settings that are configured in the **Advanced** tab of the Internet Explorer UI.

The **Internet Control Panel\Disable the Advanced Page** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

### *Internet Control Panel\Disable the Security Page*

This policy setting works in conjunction with other settings to ensure that users cannot change the settings that are configured through Group Policy. This policy setting removes the **Security** tab from the **Internet Options** dialog box. If you enable this policy setting, users cannot view and change settings for security zones, such as scripting, downloads, and user authentication. Microsoft recommends that this policy setting be enabled so that users cannot change settings that will weaken other security settings in Internet Explorer.

The **Internet Control Panel\Disable the Security Page** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

### *Offline Pages\Disable adding channels*

This policy setting removes users' ability to add channels to Internet Explorer. Channels are Web sites that are updated automatically on computers that run Internet Explorer, and the update schedule is specified by the channel provider. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content. It is a best practice to only allow a computer to download pages from the Internet when a user makes requests directly from the computer.

For these reasons, the **Offline Pages\Disable adding channels** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable adding schedules for offline pages*

This policy setting removes users' ability to specify that Web pages can be downloaded and viewed offline. This capability allows users to view Web pages when their computers are not connected to the Internet.

The **Offline Pages\Disable adding schedules for offline pages** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable all scheduled offline pages*

This policy setting disables any existing schedules that are set up to download Web pages so that they can be viewed offline. If you enable this policy, the check boxes for schedules on the **Schedule** tab of the **Web page properties** dialog box are cleared and users cannot select them. To display this tab, users click the **Tools** menu, **Synchronize**, select a Web page, then click the

**Properties** button and the **Schedule** tab. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content.

The **Offline Pages\Disable all scheduled offline pages** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable channel user interface completely*

This policy setting removes users' ability to view the Channel Bar interface. Channels are Web sites that are automatically updated on computers, and the schedule is specified by the channel provider. If you enable this policy setting, users will not be able to access the Channel Bar interface and select the **Internet Explorer Channel Bar** check box on the **Web** tab in the **Display Properties** dialog box. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content.

The **Offline Pages\Disable channel user interface completely** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable downloading of site subscription content*

This policy setting removes users' ability to download subscription content from Web sites. However, synchronization of Web page content will still occur when the user returns to a page that was previously accessed to determine if any content has been updated. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content.

The **Offline Pages\Disable downloading of site subscription content** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable editing and creating of schedule groups*

This policy setting removes users' ability to add, edit, or remove schedules for offline review of Web pages and groups of Web pages to which they subscribe. A subscription group is a favorite Web page and the Web pages that link to it. If you enable this policy, the **Add**, **Remove**, and **Edit** buttons are dimmed on the **Schedule** tab in the **Web page Properties** dialog box. To display this tab, users click **Tools** and then **Synchronize** in Internet Explorer, select a Web page, click the **Properties** button, and then click the **Schedule** tab. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content.

For these reasons, the **Offline Pages\Disable editing and creating of schedule groups** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable editing schedules for offline pages*

This policy setting removes users' ability to edit any existing schedules that are set up to download Web pages for offline review. If you enable this policy, users will not be able to display the schedule properties of pages that have been set up for offline review. No properties will display when users click **Tools**, **Synchronize** in Internet Explorer, select a Web page, and then click the **Properties** button. Users do not receive any message that states the command is unavailable. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content.

The **Offline Pages\Disable editing schedules for offline pages** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable offline page hit logging*

This policy setting removes the ability of channel providers to record how often their channel pages are viewed by users when they are offline. This policy setting is one of several that block the ability of Internet Explorer to automatically download content.

The **Offline Pages\Disable offline page hit logging** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable removing channels*

This policy setting removes users' ability to disable channel synchronization in Internet Explorer. It is a best practice to only allow a computer to download pages from the Internet when a user makes requests directly from the computer.

For this reason, the **Offline Pages\Disable removing channels** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Offline Pages\Disable removing schedules for offline pages*

This policy setting removes users' ability to clear preconfigured settings for Web pages to download for offline review. If you enable this policy setting, preconfigured Web page settings are protected. This policy setting is one of several settings that block the ability of Internet Explorer to automatically download content.

The **Offline Pages\Disable removing schedules for offline pages** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

### *Configure Outlook Express*

This policy setting allows administrators to enable and disable the ability of Microsoft Outlook® Express users to save or open attachments that can potentially contain a virus. Users cannot disable the **Configure Outlook Express** setting to stop it from blocking attachments. To enforce this policy setting, click **Enable** and select **Block attachments that could contain a virus**.

The **Configure Outlook Express** setting is configured to **Enabled** with the **Block attachments that could contain a virus** option for the two environments that are discussed in this chapter.

### *Disable Changing Advanced page settings*

This policy setting removes users' ability to change settings on the **Advanced** tab in the **Internet Options** dialog box of Internet Explorer. If you enable this policy setting, users will not be able to change advanced settings that are related to security, multimedia, and printing in the browser. Also, they will not be able to select or clear the check boxes for these options on the **Advanced** tab of the **Internet Options** dialog box. This policy setting also removes users' ability to change settings that are configured through Group Policy.

The **Disable Changing Advanced page settings** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

**Note**: If you configure the **Disable the Advanced page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to configure this policy setting because the **Disable the Advanced page** setting removes the **Advanced** tab from the **Internet Options** dialog box.

### *Disable Changing Automatic Configuration Settings*

This policy setting removes users' ability to change automatically configured settings. Administrators use automatic configuration to update browser settings periodically. If you enable this policy setting, the automatic configuration settings are dimmed in Internet Explorer. (These settings are located in the **Automatic Configuration** area of the **LAN Settings** dialog box.) This policy setting also removes users' ability to change settings that are configured through Group Policy.

**To view the LAN Settings dialog box**

1. Open the **Internet Options** dialog box, and click the **Connections** tab.
2. Click the **LAN Settings** button to view the settings.

The **Disable Changing Automatic Configuration Settings** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

**Note**: The **Disable the Connections page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) removes the **Connections** tab from Internet Explorer in Control Panel and takes precedence over this **Disable Changing Automatic Configuration Settings** configuration option. If the former setting is enabled, the latter setting is ignored.

## *Disable Changing Certificate Settings*

This policy setting removes users' ability to change certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers. If you enable this policy setting, the certificate settings in the **Certificates** area of the **Content** tab in the **Internet Options** dialog box are dimmed. This policy setting also removes users' ability to change settings that are configured through Group Policy.

The **Disable Changing Certificate Settings** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

**Note**: When this policy setting is enabled, users can still double-click the software publishing certificate (.spc) file to run the Certificate Manager Import Wizard. This wizard enables users to import and configure settings for certificates from software publishers that are not already configured in Internet Explorer.

**Note**: The **Disable the Content page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) removes the **Content** tab from Internet Explorer in Control Panel and takes precedence over this **Disable Changing Certificate Settings** configuration option. If the former setting is enabled, the latter setting is ignored.

## *Disable Changing Connection Settings*

This policy setting removes users' ability to change dial-up settings. If you enable this policy setting, the **Settings** button on the **Connections** tab in the **Internet Options** dialog box is dimmed. This policy setting also removes users' ability to change settings that are configured through Group Policy. You may want to disable this policy setting for laptop users if their travel requires them to change their connection settings.

The **Disable Changing Connection Settings** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

**Note**: If you configure the **Disable the Connections page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to configure this policy setting. The **Disable the Connections page** setting removes the **Connections** tab from the interface.

## *Disable Changing Proxy Settings*

This policy setting removes users' ability to change proxy settings. If you enable this policy setting, the proxy settings are dimmed. (The proxy settings are located in the **Proxy Server** area of the **LAN Settings** dialog box that appears when the user clicks the **Connections** tab and then the **LAN Settings** button in the **Internet Options** dialog box.) This policy setting also removes users' ability to change settings that are configured through Group Policy. You may want to disable this policy setting for laptop users if their travel requires them to change their connection settings.

The **Disable Changing Proxy Settings** setting is configured to **Enabled** only for the SSLF environment. This policy setting is not configured for the EC environment.

**Note**: If you configure the **Disable the Connections page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to configure this policy setting. The **Disable the Connections page** setting removes the **Connections** tab from the interface.

### *Do not allow AutoComplete to save passwords*

This policy setting disables automatic completion of user names and passwords in forms on Web pages, and prevents user prompts to save passwords. If you enable this policy setting, the check boxes for **User Names and Passwords on Forms** and **Prompt Me to Save Passwords** are dimmed and users are prevented from saving passwords locally. To display these check boxes, users can open the **Internet Options** dialog box, click the **Content** tab, and then the **AutoComplete** button.

The **Do not allow AutoComplete to save passwords** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

## Attachment Manager

You can configure the following prescribed user settings in the following location within the Group Policy Object Editor:

> **User Configuration\Administrative Templates\Windows Components\ Attachment Manager**

The following table summarizes the recommended Attachment Manager user configuration settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.28 Recommended Attachment Manager User Configuration Settings**

| Setting | EC computer | SSLF computer |
|---|---|---|
| Do not preserve zone information in file attachments | Disabled | Disabled |
| Hide mechanisms to remove zone information | Enabled | Enabled |
| Notify antivirus programs when opening attachments | Enabled | Enabled |

### *Do not preserve zone information in file attachments*

This policy setting allows you to manage whether Windows marks file attachments from Internet Explorer or Outlook Express with information about their zone of origin (such as restricted, Internet, intranet, or local). This policy setting requires that files be downloaded to NTFS disk partitions to function correctly. If zone information is not preserved, Windows cannot make proper risk assessments based on the zone where the attachment came from.

If the **Do not preserve zone information in file attachments** setting is enabled, file attachments are not marked with their zone information. If this policy setting is disabled, Windows is forced to store file attachments with their zone information. Because dangerous attachments are often downloaded from untrusted Internet Explorer zones such as the Internet zone, Microsoft recommends that you configure this policy setting to **Disabled** to ensure that as much security information as possible is preserved with each file.

The **Do not preserve zone information in file attachments** setting is configured to **Disabled** for both of the environments that are discussed in this chapter.

### *Hide mechanisms to remove zone information*

This policy setting allows you to manage whether users can manually remove the zone information from saved file attachments. Typically, users can either click the **Unblock** button in the file's **Property** sheet or select a check box in the **Security Warning** dialog. If the zone information is removed, users can open potentially dangerous file attachments that Windows has prevented users from opening.

When the **Hide mechanisms to remove zone information** setting is enabled, Windows hides the check box and **Unblock** button. When this policy setting is disabled, Windows displays the check box and the **Unblock** button. Because dangerous attachments are often downloaded from untrusted Internet Explorer zones such as the Internet zone, Microsoft recommends that you configure this policy setting to **Enabled** to ensure that as much security information as possible is retained with each file.

The **Hide mechanisms to remove zone information** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: To configure whether files are saved with zone information, see the previous **Do not preserve zone information in file attachments** setting.

### *Notify antivirus programs when opening attachments*

Antivirus programs are mandatory in many environments and provide a strong defense against attack.

The **Notify antivirus programs when opening attachments** setting allows you to manage how registered antivirus programs are notified. When enabled, this policy setting configures Windows to call the registered antivirus program and have it scan file attachments when they are opened by users. If the antivirus scan fails, the attachments are blocked from being opened. If this policy setting is disabled, Windows does not call the registered antivirus program when file attachments are opened. To help ensure that virus scanners examine every file before it is opened, Microsoft recommends that this policy setting be configured to **Enabled** in all environments.

The **Notify antivirus programs when opening attachments** setting is configured to **Enabled** for both of the environments that are discussed in this chapter.

**Note**: An updated antivirus program must be installed for this policy setting to function properly. Many updated antivirus programs use new APIs that are included with SP2.

## Windows Explorer

Windows Explorer is used to navigate the file system on client computers that run Windows XP Professional.

You can configure the following prescribed user settings in the following location within the Group Policy Object Editor:

> **User Configuration\Administrative Templates\Windows Components\ Windows Explorer**

The following table summarizes the recommended Windows Explorer user configuration settings. Additional information about each setting is provided in the subsections that follow the table.

**Table 4.29 Recommended Windows Explorer User Configuration Settings**

| Setting | EC computer | SSLF computer |
|---|---|---|
| Remove CD Burning features | Not configured | Enabled |
| Remove Security tab | Not configured | Enabled |

### *Remove CD Burning features*

This policy setting removes the built-in Windows XP features that allow users to burn CDs through Windows Explorer. Windows XP allows you to create and modify rewritable CDs if you have a read/write CD drive connected to your computer. This feature can be used to copy large amounts of data from a hard drive to a CD, which may then be removed from the computer.

The **Remove CD Burning features** setting is configured to **Not Configured** for the EC environment. However, this policy setting is configured to **Enabled** for the SSLF environment.

**Note**: This policy setting does not prevent CDs from being modified or created by third-party applications that use a CD writer. This guide recommends the use of software restriction policies to block the creation or modification of CDs by third-party applications. For more information, see Chapter 6, "Software Restriction Policy for Windows XP Clients."

Another way to prevent users from burning CDs is to remove the CD writers from the client computers in your environment or replace them with read-only CD drives.

### *Remove Security tab*

This policy setting disables the **Security** tab on the file and folder properties dialog boxes in Windows Explorer. If you enable this policy setting, users cannot access the **Security** tab after opening the **Properties** dialog box for all file system objects, including folders, files, shortcuts, and drives. Because the **Security** tab is inaccessible, users cannot change settings or view the list of users.

For these reasons, the **Remove Security tab** setting is **Not Configured** for the EC environment. However, this policy setting is configured to **Enabled** for the SSLF environment.

## *System*

The following figure illustrates the sections in Group Policy that will be affected by the setting changes in the System section:

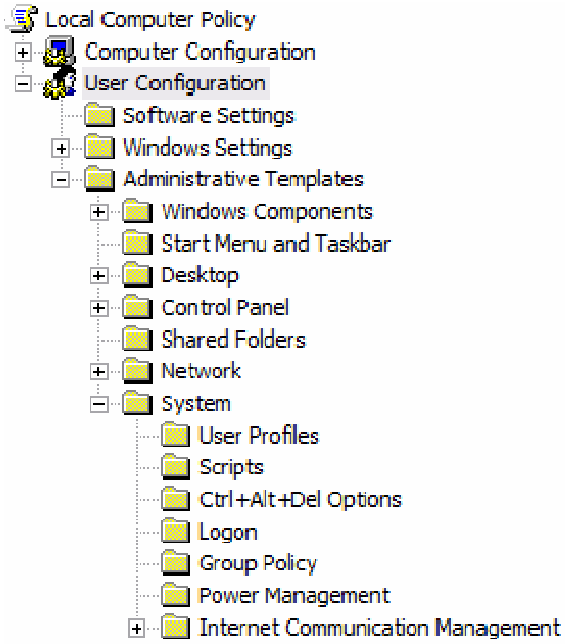


**Figure 4.7 Group Policy structure for User Configuration System**

You can configure the following prescribed setting in the following location within the Group Policy Object Editor:

**User Configuration\Administrative Templates\System**

## Prevent access to registry editing tools

The following table summarizes the recommended Registry Editor User configuration settings.

**Table 4.30 Recommended Registry Editor User Configuration Settings**

| Setting | EC computer | SSLF computer |
|---|---|---|
| Prevent access to registry editing tools | Not configured | Enabled |

This policy setting disables the Windows registry editors Regedit.exe and Regedt32.exe. If you enable this policy setting, a message will display when users try to use a registry editor that informs them that they cannot use either of these editors. This policy setting removes users' and intruders' ability to access the registry with these tools, but does not prevent access to the registry itself.

The **Prevent access to registry editing tools** setting is **Not Configured** for the EC environment. However, this policy setting is configured to **Enabled** for the SSLF environment.

## System\Power Management

You can configure the following prescribed setting in the following location within the Group Policy Object Editor:

**User Configuration\Administrative Templates\System\Power Management**

### *Prompt for password on resume from hibernate / suspend*

The following table summarizes the recommended **Prompt for password on resume from hibernate** / **suspend** configuration settings.

**Table 4.31 Recommended System\Power Management User Configuration Settings**

| Setting | EC computer | SSLF computer |
|---|---|---|
| Prompt for password on resume from hibernate / suspend | Enabled | Enabled |

This policy setting controls whether client computers in your environment are locked when they resume operational mode from a hibernated or suspended state. If you enable this policy setting, client computers are locked when they resume operational mode and users must enter their passwords to unlock them. Potentially serious security breaches can occur if this policy setting is disabled or not configured, because the client computers may be accessed by anyone.

For this reason, the **Prompt for password on resume from hibernate** / **suspend** setting is configured to **Enabled** for the two environments that are discussed in this chapter.

# Summary

This chapter described many of the most important security settings that are available in the Administrative Templates that ship with Windows XP. You can use these templates to secure the desktops and laptops that run Windows XP in your organization. When you consider security setting policies for your organization, it is important to remember the tradeoffs between security and user productivity. The goal is to protect your users from malicious programs and viruses with

a secure computing experience that allows them to fully perform their jobs without the frustrations that can be caused by overly restrictive security settings.

# More Information

The following links provide additional information about Windows XP Professional security-related topics.

- For a complete listing of all Administrative Template Group Policy settings that are available in Windows XP and Windows Server 2003, download the "Group Policy Settings Reference" workbook at http://www.microsoft.com/downloads/details.aspx?FamilyId=7821C32F-DA15-438D-8E48-45915CD2BC14.
- For information about creating your own Administrative Templates, see the white paper "Using Administrative Template Files with Registry-Based Group Policy" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx
- For information about error reporting, see the Windows Corporate Error Reporting Web site at http://www.microsoft.com/resources/satech/cer/.
- For general information about the Windows Server Update Service (WSUS), see the Windows Server Update Services Product Overview at http://www.microsoft.com/windowsserversystem/updateservices/evaluation/overview.mspx.
- For information about how to deploy WSUS, see the Deploying Microsoft Windows Server Update Services at http://technet2.microsoft.com/WindowsServer/en/Library/ace052df-74e7-4d6a-b5d4-f7911bb06b401033.mspx.
- For more information about Group Policy Management, see Enterprise Management with the Group Policy Management Console at http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.
- For more information about how to use the security settings and features in Office 2003, see Microsoft Office Assistance: Overview of Office Security at http://office.microsoft.com/en-us/assistance/HA011403061033.aspx.
- For more information about the basic intent of the policies that are listed in the various Administrative Template (ADM) and OPA files see the Office 2003 SP1 ADMs, OPAs, and Explain Text Update download, at http://www.microsoft.com/downloads/details.aspx?familyid=ba8bc720-edc2-479b-b115-5abb70b3f490&displaylang=en.
- For the Office 2003 Editions Resource Kit Tools download, which includes the "Office 2003 Policy Template Files and Deployment Planning Tools" as well as a number of other useful tools for deploying and managing Office 2003, see http://www.microsoft.com/downloads/details.aspx?FamilyID=4bb7cb10-a6e5-4334-8925-3bcf308cfbaf&DisplayLang=en.
- For more information about the Internet Explorer Administration Kit, see http://www.microsoft.com/technet/prodtechnol/ie/ieak/.

# Chapter 5: Securing Stand-Alone Windows XP Clients

## Overview

Microsoft® Windows® XP Professional–based computers that are not members of an Active Directory® directory service–based domain present some unique management challenges. This chapter discusses how to most effectively apply and manage the policy settings that are recommended in the previous chapters of this guide. The prescribed policy settings will help you ensure that stand-alone desktop and laptop computers in your organization that run Windows XP Professional are secure. The settings are applied by means of local policy, which applies to all users who log on to the client computer, including the local Administrator.

This chapter does not provide guidance for all of the available policy settings in Windows XP. However, the prescribed policy settings will provide an operating environment that is secure from most current threats and allow users to continue to use their computers. Any policy settings that you apply should be based on the security goals of your organization.

## Windows XP in a Windows NT 4.0 Domain

A specific example of a Windows XP client computer in a non-Active Directory domain environment would be a Windows XP–based computer in a Microsoft Windows NT® 4.0 domain. In such an environment, the Windows XP clients are treated as stand-alone computers. There is more management overhead in this type of environment because there is not a central location from which to manage the policy settings. Microsoft recommends that you install the Windows NT 4.0–based domain controllers with Service Pack 6a (SP6a) and the most recent updates. Windows NT 4.0 SP6a contains several updates for NTLM authentication. Without these updates, Windows XP–based computers in a Windows NT 4.0–based domain may experience domain or network connectivity and communication issues. The administrator should frequently check for updates.

Windows XP Professional provides more policy settings than previous versions of Windows, which enables you to better customize user and computer settings. Several hundred new local policy settings are available in Windows XP Professional, in addition to those already available for Windows 2000 Professional. Local policy is a powerful management feature that allows you to lock down and fine tune your desktop computers. It also introduces the possibility of many different customized scenarios. Domain administrators are made members of the local **Administrators** group on all client computers that join the domain; therefore the Windows XP client computers will only be as secure as the domain to which they belong.

Windows XP client computers in a legacy environment use a modified version of the security templates from Chapter 3, "Security Settings for Windows XP Clients" to ensure that they can communicate with the Windows NT 4.0 domain controllers. These policy settings are applied by means of the scripts that are described at the end of this chapter.

To communicate to a Windows NT 4.0 domain controller, the following policy settings are modified under **Computer Configuration\Windows Settings\Security Settings\Local Policies \Security Options**:

- **Domain member: Require strong (Windows 2000 or later) session key – Disabled**
- **Microsoft network client: Digitally sign communications (always) – Disabled**

These policy settings are preconfigured in the legacy client security template files that are included with this guide.

# Local Group Policy Object Settings

Each Windows XP Professional operating system has one Local Group Policy object (LGPO). The policy settings are applied to the LGPO manually with the Group Policy Object Editor or through scripts. LGPOs contain fewer policy settings than domain–based GPOs, particularly under Security Settings. LGPOs do not support Folder Redirection, Remote Installation Service, or Group Policy Software Installation when they are configured as stand-alone client computers, but you can use them to provide a secure operating environment on such computers.

The following table shows which Group Policy snap-in extensions open when the Group Policy snap-in is focused on an LGPO.

**Table 5.1 Group Policy Snap-in Extensions**

| Group Policy snap-in extension | Available in LGPO |
|---|---|
| Software Installation | No |
| Scripts | Yes |
| Security Settings | Yes |
| Administrative Templates | Yes |
| Folder Redirection | No |
| Internet Explorer Maintenance | Yes |
| Remote Installation Service | No |

## *Account Policies*

Account policies include Password policy, Account Lockout policy, and Kerberos policy settings. Password policy can help secure most environments through its ability to require password complexity and frequent password changes. Account Lockout policy provides the ability to automatically disable an account after a series of unsuccessful logon attempts. Kerberos policy settings determine Kerberos-related attributes of domain user accounts, such as the **Maximum lifetime for user ticket** and **Enforce user logon restrictions settings**. However, these policy settings are not used for stand-alone client computers because they do not participate in a domain.

Typically, account policies are set at the domain level and are thereby configured for domain client computers. For stand-alone Windows XP client computers, these policy settings need to be applied locally, similar to the policy settings that are described in Chapter 2, "Configuring the Active Directory Domain Infrastructure" of this guide.

## *Local Policies*

Local policies, under **Computer Configuration\Windows Settings\Security Settings**, will be applied to the client computer with the templates that are described in Chapter 3, "Security Settings for Windows XP Clients" of this guide. A combination of those templates and the ones that were created for the stand-alone client computers are used; you can automate the application of the security templates by means of scripts that you can apply to multiple computers in the environment. The next section describes the process for creating and deploying local policies.

# Importing Security Templates into Windows XP

There are several different templates that you can use to configure the stand-alone client computer by means of a script; you should use a template that supports the security requirements of the client. The previous section discussed local policy settings and how the Group Policy Object Editor is used to configure them. You can use the provided templates to automate the configuration process for many client computers in either a network-connected or stand-alone environment. This section will explain the process of how to automate the configuration of security policies.

## *Configuration*

A security template is a file that represents a security configuration. To apply security templates to a local computer, you can import them into the LGPO. The templates that were created in Chapter 3, "Security Settings for Windows XP Clients" will be used to configure the local policies. The administrator will use the Microsoft Management Console (MMC) Security Configuration and Analysis snap-in, the Security Templates snap-in, and Secedit.exe to create the account policies and merge the two security templates on the stand-alone computer.

### Creating a Security Database

To automate the process of importing security settings on a stand-alone client computer, you must create a reference database to write to the local security policy. The baseline database was created with the MMC Security Configuration and Analysis snap-in. The following steps were used to create the XP Default Security.sdb database. The database used the Setup security.inf file as the template to establish the default policy settings for the stand-alone client computer.

**To create a new default security database**

1. On the **Start** menu, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **New** to create a new console.
3. On the **File** menu, click **Add/Remove Snap-in**. Then click the **Stand-alone** tab in the **Add/Remove snap-in properties** dialog box and click **Add**.
4. Select **Security Configuration and Analysis**, click **Add**, click **Close**, and then click **OK**.
5. Right-click the **Security Configuration and Analysis** scope item and then click **Open Database**.
6. Type a new database name (XP Default Security), and then click **Open**.
7. Select a security template to import (**setup security.inf**), and then click **Open**.
8. Right-click the **Security Configuration and Analysis** scope item, and then click **Configure Computer Now**.

9. In the **Configure System** dialog box, type the name of the log file you wish to use and then click **OK**.

This process creates a database file with the default security settings that will be used in the automation process. Copy the security database to the same folder to which you copied the scripts and the information files. The custom scripts will be used to configure the database, which will configure the local security policy. The administrator can use similar steps to create a custom database instead of using the one that is provided with this guide.

## Creating Custom Templates

You can use the MMC Security Templates snap-in to define security policy settings in the templates, which you can then apply to a local computer. The following steps were performed to create the Standalone-EC-Account.inf and Standalone-SSLF-Account.inf templates by using the policy settings from the Account Policy tables in Chapter 2, "Configuring the Active Directory Domain Infrastructure."

**To create a custom template**

1. Click **Start**, **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **New** to create a new console.
3. On the **File** menu, click **Add/Remove Snap-in**. Then click the **Stand-alone** tab in the **Add/Remove snap-in properties** box and click **Add**.
4. Click **Security Templates**, click **Add**, click **Close**, and then click **OK**.
5. Open **Security Templates**.
6. Select the default folder to store the new template, and then click **New Template**.
7. In the **Template name** text box, type the name for your new security template.
8. In the **Description** text box, type a description of your new security template, and then click **OK**.
9. In the console tree, double-click the new security template to display the security areas and then navigate until the policy setting you want to configure displays in the details pane.
10. In the details pane, right-click the policy setting you want to configure and then click **Properties**.
11. In the **Properties** dialog box, select the **Define this policy setting in the template** check box, edit the settings, and then click **OK**.

After the files are created, you can find them under **%windir%\security\templates**. Copy the security templates to the same folder in which you created the Security database to run the scripts. These files will be used in the next phase to automate the import of the templates.

# *Applying the Policy*

The Secedit.exe tool is useful when you need to configure security on multiple computers. You can call the Secedit.exe tool at a command prompt, from a batch file, or from the automatic task scheduler to automatically create and apply templates. You can also run it dynamically from a command prompt. The scripts that are provided with this guide use the Secedit.exe tool to merge and apply local policy to client computers.

## Manually Applying the Local Policy

To apply all of the policy settings in the stand-alone security template's .inf file that is included with this guide, use the MMC Security Configuration and Analysis snap-in instead of the Local Computer Policy snap-in. It is not possible to import the security template with the Local

Computer Policy snap-in because it does not allow you to apply security policy settings for system services.

To import and apply the security template, use the Security Configuration and Analysis snap-in to complete the steps in the following procedures.

**To import a security template**

1. Launch the MMC Security Configuration and Analysis snap-in.
2. Right-click the **Security Configuration and Analysis** scope item.
3. Click **Open Database**.
4. Type a new database name, and then click **Open**.
5. Select a security template (.inf file) to import, and then click **Open**.

All the policy settings in the template will be imported, after which they can be reviewed or applied.

**To apply the policy settings**

1. Right-click the Security Configuration and Analysis scope item.
2. Select **Configure Computer Now**.
3. In the **Configure Computer Now** dialog box, type the name of the log file you wish to use, and then click **OK**.

You will have to import both templates for each environment. All pertinent policy settings from the security template will be applied to the client computer's local policy. The following sections describe the policy settings that are applied through local policy.

# Secedit

This tool configures and analyzes system security; to do so, it compares your current configuration to at least one template. The syntax for using the Secedit.exe tool is as follows:

**secedit** /**configure** /**db** *<FileName>* [/**cfg** *<FileName>*] [/**overwrite**][/**areas** *<Area1>* *<Area2>* ...]
**[**/**log** *<FileName>*] [/**quiet**]

The following list explains the parameters of the Secedit.exe tool.

- /**db** *<FileName>*. Specifies the database that is used to perform the security configuration.
- /**cfg** *<FileName>*. Specifies a security template to import into the database before the computer is configured. Security templates are created using the Security Templates snap-in.
- /**overwrite**. Specifies that the database should be emptied before the security template is imported. If this parameter is not specified, the policy settings in the security template will accumulate in the database. If this parameter is not specified and policy settings in the template you wish to import conflict with existing policy settings in the database, the settings in the template will apply.
- /**areas** *<Area1>* *<Area2>*. Specifies the security areas to be applied to the system. If this parameter is not specified, all security policy settings that are defined in the database are applied to the system. To configure multiple areas, separate each area with a space. The following table shows the security areas that are supported.

**Table 5.2 Security Areas**

| Area name | Description |
|---|---|
| SECURITYPOLICY | Includes Account policies, Audit policies, event log settings, and security options. |
| GROUP_MGMT | Includes Restricted Group settings. |
| USER_RIGHTS | Includes user rights assignment settings. |
| REGKEYS | Includes registry permissions. |
| FILESTORE | Includes file system permissions. |
| SERVICES | Includes system service settings. |

- /**log** *<FileName>*. Specifies a file in which to log the status of the configuration process. If not specified, configuration data is logged in the Scesrv.log file, which is located in the **%windir%\security\logs** directory.
- /**quiet**. Specifies that the configuration process should occur and not prompt the user.

## Automated Scripts

It is always easier to use a script to apply identical policy settings to many client computers. You can use the Secedit.exe tool described earlier in this chapter to automate the application of local policy with a simple script. Copy the script and all associated files to a subdirectory on the local hard disk, and then execute the script from the subdirectory.

You can use the following script to import security templates into the LGPO to secure the stand-alone Windows XP client computers in your environment.

**Important:** Be certain that the security database file **XP Default Security.sdb** is not marked Read Only. For the following script to function correctly it must be able to make changes to that file.

```
REM (c) Microsoft Corporation 1997-2005

REM Script for Securing Stand-Alone Windows XP Client Computers
REM
REM Name:         Standalone-EC-Desktop.cmd
REM Version:      2.0

REM This CMD file provides the proper secedit.exe syntax for importing the
REM security policy for a secure stand-alone Windows XP desktop client
REM computer. Please read the entire guide before using this CMD file.



REM Resets the Policy to Default Values
secedit.exe /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb
/verbose



REM Sets the Account Settings
```

```
secedit.exe /configure /db "XP Default Security.sdb" /cfg "Standalone-EC-
Account.inf" /overwrite /quiet


REM Sets the Security Settings
secedit.exe /configure /db "XP Default Security.sdb" /cfg "EC-Desktop.inf"


REM Deletes the Shared Folder
reg delete
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\D
elegateFolders\{59031a47-3f72-44a7-89c5-5595fe6b30ee}" /f

REM Updates the Local Policy
gpupdate.exe /force
```

The following tables list the scripts and associated files that are included with this guide. For each environment, there are files for both desktop and laptop client computers.

**Table 5.3 Stand-Alone Scripts and Files**

| Script and file names | Description |
|---|---|
| Standalone-EC-Desktop.cmd | A stand-alone script that is used to set Enterprise Client policy on desktop client computers. |
| Standalone-EC-Laptop.cmd | A stand-alone script that is used to set Enterprise Client policy on laptop client computers. |
| Standalone-SSLF-Desktop.cmd | A stand-alone script that is used to set Specialized Security – Limited Functionality policy on desktop client computers. |
| Standalone-SSLF-Laptop.cmd | A stand-alone script that is used to set Specialized Security – Limited Functionality policy on laptop client computers. |
| Standalone-EC-Account.inf | The Enterprise Client Account Policy template. |
| Standalone-SSLF-Account.inf | The Specialized Security – Limited Functionality Account Policy template. |
| EC-Desktop.inf | The Enterprise Client Security template for desktop client computers. |
| EC-Laptop.inf | The Enterprise Client Security template for laptop client computers. |
| SSLF-Desktop.inf | The Specialized Security – Limited Functionality template for desktop client computers. |
| SSLF-Laptop.inf | The Specialized Security – Limited Functionality template for laptop client computers. |
| XP Default Security.sdb | The default policy database. |

**Table 5.4 Legacy Scripts and Files**

| Script and File Names | Description |
|---|---|
| Legacy-EC-Desktop.cmd | A legacy script that is used to set Enterprise Client policy on desktop client computers. |
| Legacy-EC-Laptop.cmd | A legacy script that is used to set Enterprise Client policy on laptop client computers. |
| Legacy-SSLF-Desktop.cmd | A legacy script that is used to set Specialized Security – Limited Functionality policy on desktop client computers. |
| Legacy-SSLF-Laptop.cmd | A legacy script that is used to set Specialized Security – Limited Functionality policy on laptop client computers. |
| Legacy-EC-Account.inf | The Legacy Enterprise Account Policy template. |
| Legacy-SSLF-Account.inf | The Legacy Specialized Security – Limited Functionality Account Policy template. |
| Legacy-EC-Desktop.inf | The Legacy Enterprise Client Security template for desktop client computers. |
| Legacy-EC-Laptop.inf | The Legacy Enterprise Client Security template for laptop client computers. |
| Legacy-SSLF-Desktop.inf | The Legacy Specialized Security – Limited Functionality template for desktop client computers. |
| Legacy-SSLF-Laptop.inf | The Legacy Specialized Security – Limited Functionality template for laptop client computers. |
| XP Default Security.sdb | The default policy database.<br>**Note**: Ensure the database has write privileges. It cannot be set to read-only. |

# Summary

Windows XP local policy is a very useful way to provide consistent security policy settings to Windows XP systems that are not members of an Active Directory domain. To deploy local policy effectively, ensure that you are aware of how it can be applied, that all of your client computers are configured with the appropriate settings, and that you have defined appropriate security for each computer in your environment.

# More Information

The following links provide additional information about Windows XP Professional security-related topics.

- For more information about the Security Configuration Manager, see http://technet2.microsoft.com/WindowsServer/en/Library/74d8fed6-cf2f-4ba4-94f3-fc95bad914b01033.mspx.
- For more information about Windows Server 2003 Group Policy, see http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.mspx.
- For information about troubleshooting Group Policy in Windows Server, see the "Troubleshooting Group Policy in Microsoft Windows Server" whitepaper at http://www.microsoft.com/downloads/details.aspx?FamilyId=B24BF2D5-0D7A-4FC5-A14D-E91D211C21B2.
- For more information about Troubleshooting Group Policy application problems, see Knowledge Base article 250842 at http://support.microsoft.com/default.aspx?scid=250842.
- For more information about security tools and checklists, see Microsoft Security Tools at http://www.microsoft.com/technet/security/tools/default.mspx.
- For information about How To Identify Group Policy Objects in the Active Directory and SYSVOL, see Knowledge Base article 216359 at http://support.microsoft.com/default.aspx?scid=216359.
- For information about The role of Administrative Templates, see the Web page at http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/adminad.mspx.

# Chapter 6: Software Restriction Policy for Windows XP Clients

## Overview

Software restriction policy provides administrators with a way to identify software and control its ability to run on local computers. This tool can help protect computers that run Microsoft® Windows® XP Professional against known conflicts and safeguard them against malicious software such as viruses and Trojan horse programs. Software restriction policy integrates fully with the Active Directory® directory service and Group Policy. You can also use it on stand-alone computers.

This chapter has a different structure than the previous chapters in this guide because of the way software restriction policy works. The previous chapters provided recommendations about how to configure Group Policy setting options. Software restriction policy requires an administrator to define the applications that are allowed to run on the client computers in your environment and to then determine the restrictions that the policy will apply to the clients.

When you implement software restriction policy, the first decision you must make is whether the default security level will be **Unrestricted** or **Disallowed**. If the default security level is **Unrestricted**, then all software will be allowed to run and you will need to configure additional rules to block specific applications. The more secure approach is to configure the default security level to **Disallowed**, which means no software will be allowed to run, and then configure additional rules to allow specific applications. You can apply software restriction policy to multiple computers through domain–based Group Policies or to individual computers through local Group Policy.

**Important**: It is important that you thoroughly test all of the policy settings that are discussed in this guide before you deploy them to production systems, especially software restriction policy settings. Mistakes in the design or implementation of this feature can cause considerable user frustration.

Software restriction policy provides a number of ways to identify software, as well as a policy–based infrastructure to enforce rules on how the identified software may run. Computer users must comply with the guidelines that are established in the software restriction policy by the administrator in their environment.

You can use software restriction policy to accomplish the following:

- Control what software may run on the client computers in your environment.
- Restrict user access to specific files on multi-user computers.
- Decide who may add trusted publishers to client computers.
- Define whether the policies affect all users or a subset of users on the client computers.
- Prevent executable files from running on your local computers based on policies that are set at a computer, OU, site, or domain level.

# Software Restriction Policy Architecture

Software restriction policy provides the following powerful features:

- **Policy enforcement that is either domain–based or local computer–based**. Administrators create the policy and then define which applications are trusted and which are not. The policy is enforced at run time and users do not receive prompts that allow them to choose whether to run executable files.
- **Policy that applies to more than just binary executable files**. The definition of what constitutes software is ambiguous. Software restriction policy provides control over Microsoft Visual Basic® Scripting Edition (VBScript), JScript®, and other scripting languages. It also integrates with the Windows Installer feature to provide control over which packages can be installed on client computers. This feature includes an application programming interface (API) that you can use to coordinate the policy runtime with other runtimes.
- **Policy that is scalable**. Because it is implemented through Group Policy, software restriction policy can be effectively implemented and managed across domains that consist of tens of thousands of computers.
- **Policy that is flexible**. Administrators have the flexibility to prohibit unauthorized scripts, to regulate Microsoft ActiveX® controls, and to tightly lock down client computers.
- **Policy that enables strong cryptography to identify software**. Software restriction policy can identify software using hashes or digital signatures.

Software restriction policy implementation includes three phases:

1. The administrator or a delegated authority creates the policy with the Microsoft Management Console (MMC) Group Policy snap-in for the Active Directory container site, domain, or OU. Microsoft recommends that you create a separate Group Policy object (GPO) for software restriction policy.

   **Note**: To create a new software restriction policy for a local stand-alone computer, you must be a member of the **Administrators** group on the local computer. To configure these policy settings, click **Windows Settings**, **Security Settings**, and then **Software Restriction Policy**.
2. The computer-level policy is downloaded and takes effect after you start the computer. User policies take effect when the user logs on to the system or domain. To update the policy, execute the **gpupdate.exe /force** command.
3. When a user starts an executable file such as an application or script, the policy determines whether it can run according to its precedence rules.

## *Unrestricted or Disallowed Settings*

A software restriction policy consists of two parts:

- A default rule that specifies which programs may run.
- An inventory of exceptions to the default rule.

You can set the default rule that is used to identify software to either **Unrestricted** or **Disallowed**—which allow you to either run or not run all software, respectively.

If you set the default rule to **Unrestricted**, an administrator can define exceptions or a set of programs that are not allowed to run. Use the **Unrestricted** default setting in an environment with loosely managed client computers. For example, you can restrict users' ability to install a program that will conflict with existing programs by creating a rule to block it.

A more secure approach is to set the default rule to **Disallowed** and then allow only a specific set of programs to run. The **Disallowed** default setting requires an administrator to define all the rules for each application and ensure that users have the correct security policy settings on their

computers to access the applications that they are allowed to run. The **Disallowed** default setting is the more secure approach for organizations that want to protect Windows XP client computers.

# Four Rules to Identify Software

Rules in a software restriction policy identify one or more applications and specify whether they are allowed to run. The enforcement engine in Windows XP queries the policy's rules before applications are allowed to run. To create a rule, you need to identify applications and then categorize them as exceptions to the **Disallowed** default setting. Each rule can include comments to describe its purpose.

A software restriction policy uses the following four rules to identify software:

- **Hash Rule**. Uses a cryptographic fingerprint of the executable file.
- **Certificate Rule**. Uses a digitally signed certificate from a software publisher for the .exe file.
- **Path Rule**. Uses the local, Universal Naming Convention (UNC), or registry path of the .exe file location.
- **Zone Rule**. Uses the Internet Zone where the executable file originated (if it was downloaded using Microsoft Internet Explorer).

## The Hash Rule

A hash is a digital fingerprint that uniquely identifies a software program or executable file even if the program or executable file is moved or renamed. Administrators can use a hash to track a particular version of an executable file or program that they may not want users to run.

With a hash rule, software programs remain uniquely identifiable because the hash rule match is based on a cryptographic calculation that involves the contents of the file. The only file types that are affected by hash rules are those that are listed in the **Designated File Types** section of the details pane for **Software Restriction Policies**.

Hash rules work effectively in a static environment. If software in your environment is upgraded, the hash needs to be recalculated for each updated executable file. Hash rules work very well in environments that experience infrequent software changes or upgrades.

A hash rule consists of the following three pieces of data, separated by colons:

- The MD5 or SHA-1 hash value
- The file length
- The hash algorithm ID number

Digitally signed files use the hash value that is contained in the signature, which may be MD5 or SHA-1. Executable files that are not digitally signed use an MD5 hash value.

Hash rules are formatted as follows:

```
[MD5 or SHA1 hash value]:[file length]:[hash algorithm id]
```

The following hash rule example is for a 126-byte file with contents that match the MD5 hash value (7bc04acc0d6480af862d22d724c3b049) and the hash algorithm (denoted by the hash algorithm identifier 32771):

```
7bc04acc0d6480af862d22d724c3b049:126:32771
```

Each file that the administrator wants to restrict or allow needs to contain a hash rule. When software is updated, the administrator must create a new hash rule for each application because the hash values for the original executable files will not match those of the new files.

Complete the steps in the following procedure to create a hash rule for an executable file.

**To create a hash rule for an existing executable file**

1. On the Group Policy Object Editor tool bar, click **Windows Settings**, **Security Settings**, **Software Restriction Policy**, and then right-click **Additional Rules**.
2. Click **New Hash Rule** on the shortcut menu.

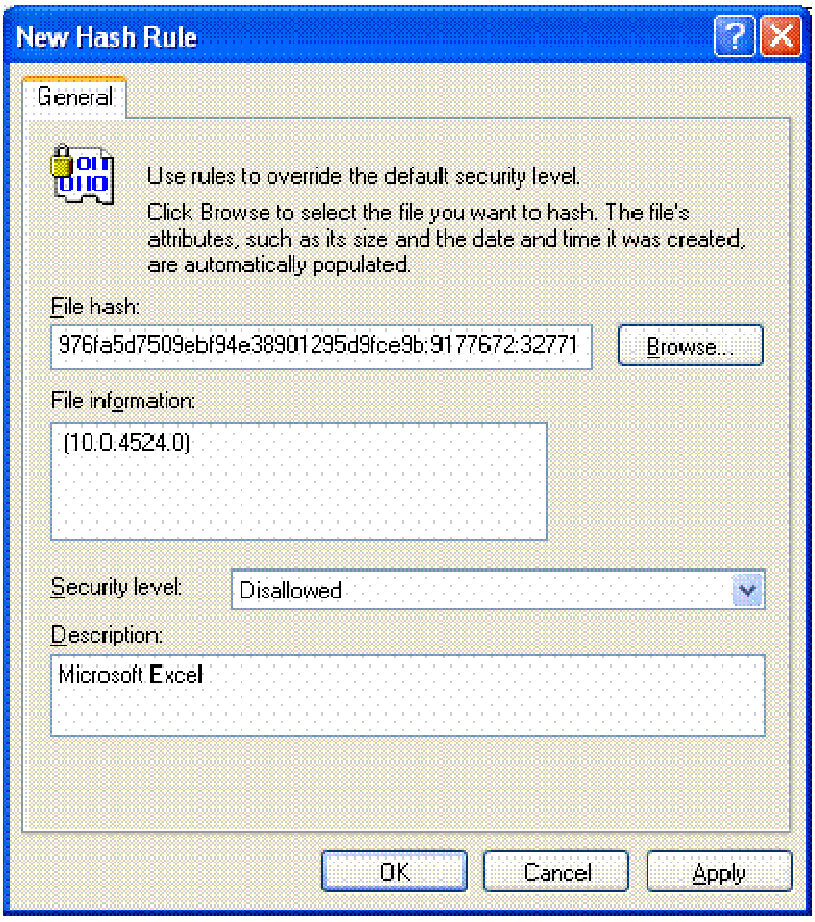


**Figure 6.1 The New Hash Rule dialog box**

3. Click **Browse** to select the file for which you want to create a hash rule. In this example, the executable file is **Excel.exe**. The new file hash value displays in the **File Hash:** box, and the application version displays in the **File Information:** box.
4. Select the default security level setting that you want for this rule. The options are:
   - **Disallowed**
   - **Unrestricted**

# The Certificate Rule

A certificate rule specifies that a software publisher's certificate (used for code-signing) must exist before a program is allowed to run. For example, an administrator can require signed certificates for all scripts and ActiveX controls. Allowable sources that comply with the certificate rule include:

- A commercial certificate authority (CA), such as VeriSign.
- A Microsoft Windows 2000/Windows Server™ 2003 public key infrastructure (PKI).
- A self-signed certificate.

A certificate rule is a strong software identification method because it uses signed hashes in the signature of the signed file to match files, regardless of name or location. Unfortunately, few software vendors use code-signing technology, and even those that do typically sign a small percentage of the executable files that they distribute. For these reasons, certificate rules are generally used for a few specific application types such as ActiveX controls or internally developed applications. For example, this guide recommends that organizations digitally sign scripts that are used to manage computers and users so that all unsigned scripts can be blocked. A hash rule can be used to identify exceptions to a certificate rule.

## *Enabling Certificate Rules*

Certificate rules are not enabled by default. Complete the steps in the following procedure to enable certificate rules.

**To enable certificate rules**

1. Open the GPO in the Group Policy Object Editor.
2. In the console tree, click **Security Options**.
3. In the details pane, double-click **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies**.
4. Click **Enabled** to make the certificate rules available.

For detailed instructions about how to digitally sign files, see the “Step-by-Step Guide to Digitally Signing Files with Test Certificates” section of the "Using Software Restriction Policies to Protect Against Unauthorized Software" at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx.

Many commercial Web sites have their software code-signed by a commercial certification authority (CA). These certificates are usually valid from one to several years. When you use certificate rules, be aware that the certificates carry expiration dates. You may be able contact the software publisher to find out more information about the expiration period for a published certificate. When you receive a certificate from a commercial CA, you can export it to a file to create a certificate rule. Complete the steps in the following procedure to export a certificate.

### To export a certificate

1. Select the trusted publisher that will issue the certificate. In this example, the certificate publisher is Microsoft MSN®.

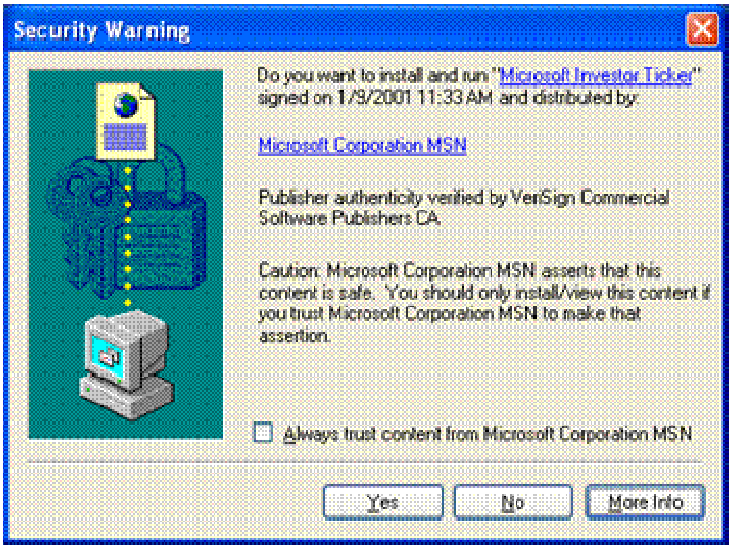


**Figure 6.2 The Security Warning dialog box that shows the trusted publisher**

2. Click the **Details** tab and then **Copy to File...** to copy this certificate to a file and use it to create a certificate rule.

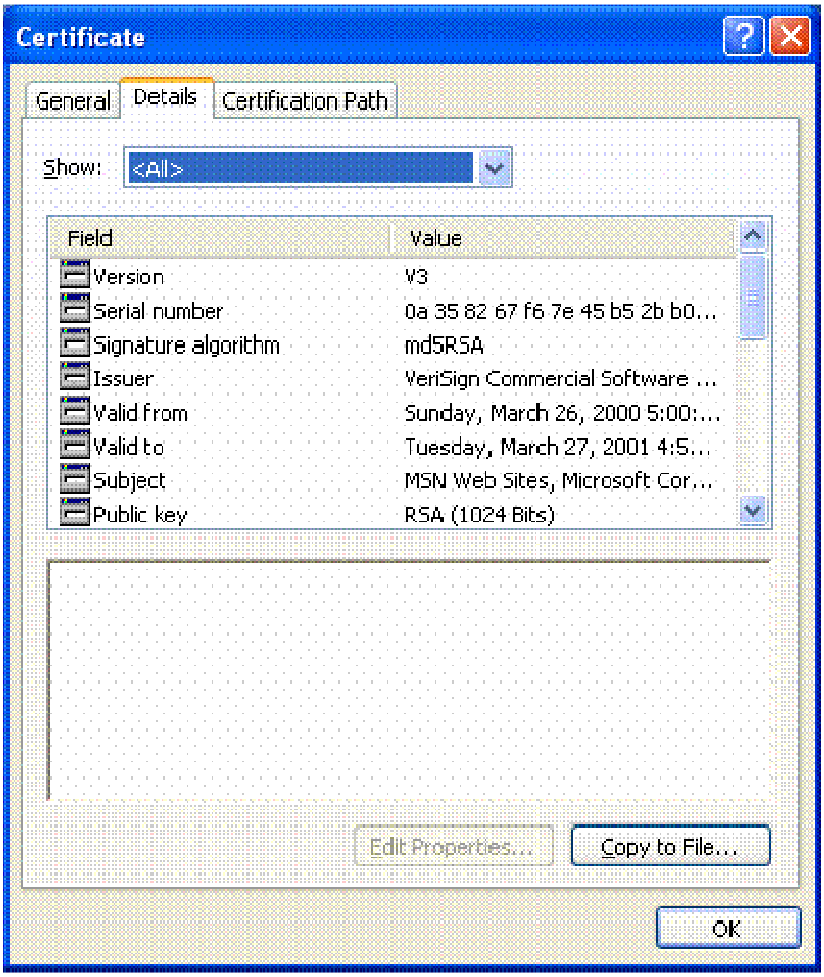


**Figure 6.3 The Details tab of the Certificate dialog box**

3. The **Certificate Export Wizard** welcome page will display. Click **Next** to continue.

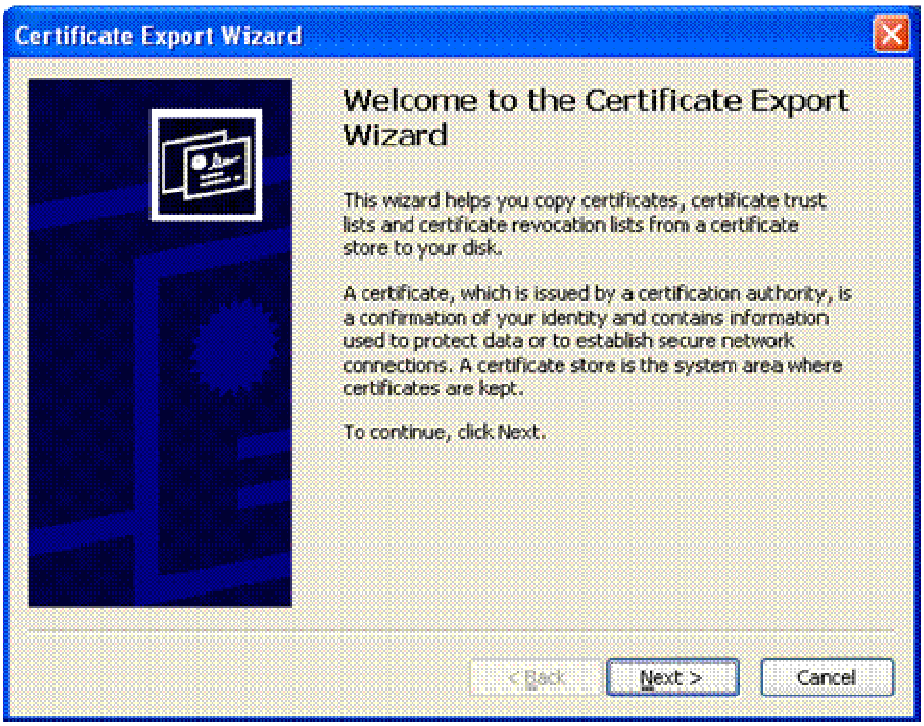


**Figure 6.4 The Certificate Export Wizard welcome page**

4. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)** and click **Next** to create the certificate file with a (.cer) extension.

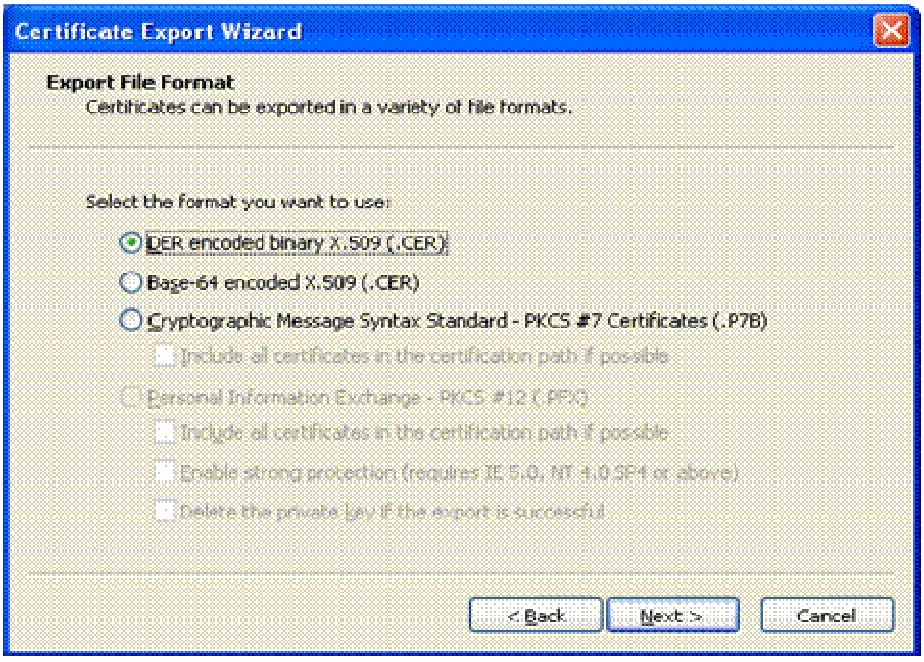


**Figure 6.5 The Certificate Export Wizard, Export File Format page that shows the selected encoding method**

5. On the **File to Export** page, designate a descriptive certificate rule file name. The certificate will be saved to whatever location you select with whatever file name you choose.

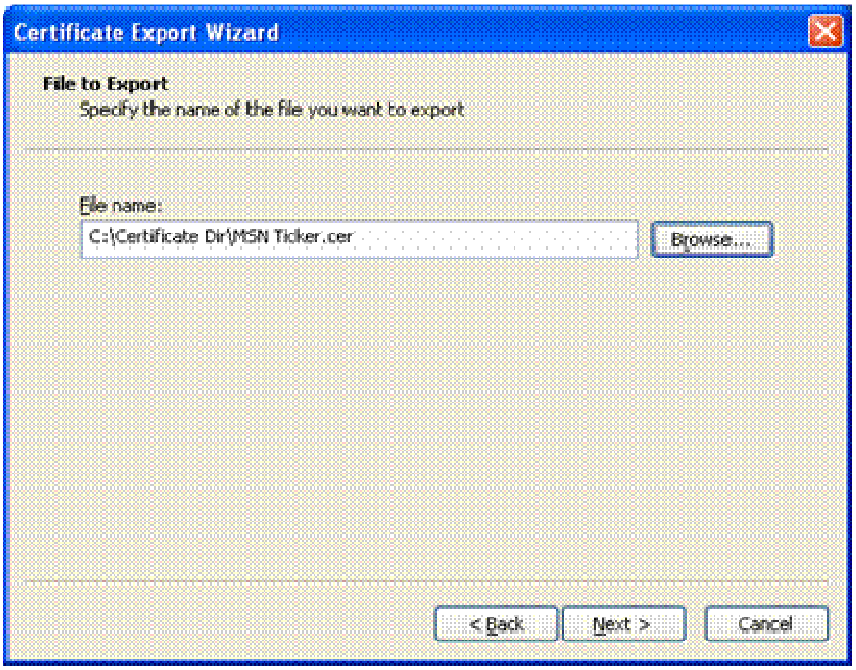


**Figure 6.6 The Certificate Export Wizard, File to Export page showing an example file name**

6. The **Completing the Certificate Export Wizard** page will display the certificate file's specified settings. Review the settings and click **Finish** to export the file.


**Figure 6.7 The Certificate Export Wizard Completion page that shows the specified settings**

# The Path Rule

A path rule specifies either a folder or a fully qualified path to a program. When a path rule specifies a folder, it matches any program that is contained in that folder and any programs that are contained in subfolders of that folder. Path rules support both local and UNC paths.

The administrator must define all directories from which a specific application will be launched in the path rule. For example, if a desktop shortcut is used to launch an application, the path rule must specify both the executable file and the shortcut paths to run the application. If a user attempts to run an application with only a partial path rule, the **Software Restricted** warning will display.

Many applications use the *%ProgramFiles%* variable to install files on the hard drive of Windows XP–based computers. Unfortunately, some applications are hard-coded to copy files to the **C:\Program Files** subdirectory, and will do so even if this variable is set to another directory on a different drive. Remember this limitation when you create and test path rules.

## *Using Environment Variables in Path Rules*

You can define a path rule to use environment variables. Because path rules are evaluated in the client environment, environment variables allow an administrator to adapt a rule to a particular user's environment.

The following two examples show instances of how to apply environment variables to a path rule.

- "%UserProfile%" matches **C:\Documents and Settings*<User>*** and all subfolders under this directory.
- "%ProgramFiles%\<*Application*>" matches **C:\Program Files*<Application>*** and all subfolders under this directory.

**Note**: Environment variables are not protected by access control lists (ACLs). There are two types of environment variables, **User** and **System**. Users who are able to start a command prompt can redefine the **Users** environment variable to a different path. Only users in the **Administrators** group can change the **System** environment variable.

Although the two preceding examples are very useful, you may want to consider other available environment variables. For a complete list, see the "Command shell overview" at http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntcmds_shelloverview.mspx.

## *Using Wildcards in Path Rules*

A path rule can incorporate the "?" and "*" wildcards. The following examples show wildcards that are applied to different path rules:

- **\\DC – ??\login$** matches **\\DC – 01\login$**, **\\DC – 02\login$**, and so on.
- ***\Windows** matches **C:\Windows**, **D:\Windows**, **E:\Windows**, and all subfolders under each directory.
- **C:\win*** matches **C:\winnt**, **C:\windows**, **C:\windir**, and all subfolders under each directory.
- ***.vbs** matches any application that has this extension in Windows XP Professional.
- **C:\Application Files*.*** matches all application files in the specific subdirectory.

## *Registry Path Rules*

Many applications store paths to their installation folders or application directories in the Microsoft Windows registry. Some applications can be installed anywhere on the file system. To locate them, you can create a path rule to look up their registry keys.

These locations may not be easily identified using specific folder paths, such as **C:\Program Files\Microsoft Platform SDK**, or environment variables, such as **%ProgramFiles%\Microsoft Platform SDK**. However, if the program stores its application directories in the registry, you can create a path rule that will use the value that is stored in the registry, such as:

**%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PlatformSDK\Directories\ Install Dir%**

This type of path rule, called a registry path rule, is formatted as follows:

%*<Registry Hive>**<Registry Key Name>**<Value Name>*%

**Note**: Any registry path rule suffix should not contain a \ character immediately after the last % sign in the rule. The registry hive name must be written completely; abbreviations will not work.

When the default rule is set to **Disallowed**, four registry path rules are set up so that the operating system has access to system files. These registry path rules are created as a safeguard—so that you do not lock yourself and all other users out of the system—and are set to **Unrestricted**. These rules should only be modified or deleted by advanced users. The registry path rule settings are:

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SystemRoot%*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SystemRoot%\System32*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\ProgramFilesDir%

### *Path Rule Precedence*

When there are multiple path rules that match, the most specific rule takes precedence over the others. The following set of paths is ordered from highest precedence (most specific match) to lowest precedence (most general match):

- Drive:\Folder1\Folder2\FileName.Extension
- Drive:\Folder1\Folder2*.Extension
- *.Extension
- Drive:\Folder1\Folder2\
- Drive:\Folder1\

## Zone Rule

You can use a zone rule to identify software that is downloaded from any of the following zones that are defined in Internet Explorer:

- Internet
- Intranet
- Restricted Sites
- Trusted Sites
- My Computer

The current version of the Internet zone rule applies only to Windows Installer (*.msi) packages. Also, this rule does not apply to software that is downloaded through Internet Explorer. All other

file types that are affected by zone rules are listed in the Designated File Types table later in this chapter. One list of designated file types is shared by all zone rules.

## Rule Recommendations

Use the information in the following table to determine which type of rule is best suited for an application's users and environment.

**Table 6.1 Determining the Best Rule for a Given Application**

| Task | Recommended rule |
|---|---|
| Allow or disallow a specific program version. | **Hash rule**<br>Browse to the file to create a hash rule. |
| Identify a program always installed in the same place. | **Path rule with environment variables**<br>%ProgramFiles%\Internet Explorer\iexplore.exe |
| Identify a program that can be installed anywhere on client computers. | **Registry path rule**<br>%HKEY_LOCAL_MACHINE\SOFTWARE\ ComputerAssociates\InoculateIT\6.0\Path\HOME% |
| Identify a set of scripts on a central server. | **Path rule**<br>\\SERVER_NAME\Share |
| Identify a set of scripts on a set of servers. For example, DC01, DC02, and DC03. | **Path rule with wildcard**<br>\\DC??\Share |
| Disallow all .vbs files, except those in a login script directory. | **Path rule with wildcard**<br>*.VBS set to **Disallowed**<br>\\LOGIN_SRV\Share*.VBS set to **Unrestricted** |
| Disallow a file installed by a virus that is always called Flcss.exe. | **Path rule**<br>Flcss.exe set to **Disallowed** |
| Identify a set of scripts that can be run anywhere. | **Certificate rule**<br>Use a certificate to digitally sign the scripts. |
| Allow software to be installed from trusted Internet zone sites. | **Zone rule**<br>Set **Trusted Sites** to **Unrestricted**. |

## Software Restriction Policy Precedence Rules

Rules are evaluated in a specific order. The rules that more specifically match a program take precedence over rules that more generally match the same program. If two identical rules with differing security levels are established for the same software, the rule with the highest security level takes precedence. For example, if two hash rules—one with the security level **Disallowed** and one with the security level **Unrestricted**—are applied to the same software program, the rule with the security level **Disallowed** takes precedence, and the program will not run. The following list defines the precedence order for the rules, from the most specific to the least specific:

1. Hash rule
2. Certificate rule
3. Path rule

4. Zone rule
5. Default rule

# Software Restriction Policy Options

This section discusses the various enforcement options that influence the way a software restriction policy functions. These options alter the way Microsoft Authenticode® trust settings are enforced for digitally signed files. There are two enforcement options: Dynamic-link library (DLL) checking and Skip Administrators.

## *DLL Checking*

Most programs consist of an executable file and many supporting DLLs. By default, software restriction policy rules are not enforced on DLLs. This default setting is recommended for most customers for the following three reasons:

- If the main executable file is disallowed the program is prevented from running, so there is no need to disallow the constituent DLLs.
- DLL checking degrades system performance because it has to check all libraries that are linked to the application. For example, if a user runs 10 programs during a logon session, the software restriction policy evaluates each program. With DLL checking turned on, the software restriction policy evaluates each DLL load within each program. If each program uses 20 DLLs, this configuration would result in 10 executable program checks plus 200 DLL checks—which would require the software restriction policy to perform 210 evaluations. A program such as Internet Explorer consists of an executable file (iexplore.exe) and many supporting DLLs.
- If the default security level is set to **Disallowed**, the system is forced to not only identify the main executable file before it is allowed to run but also all of the .exe file's constituent DLLs, which places added burden on the system.

Because viruses primarily target executable files, some specifically target DLLs. Therefore, DLL checking is the recommended option when you want the highest possible assurance for the programs running in your environment.

To ensure that a program does not contain a virus, you can use a set of hash rules that identify the executable file and all of its constituent DLLs.

**To turn off the DLL Checking option**

- When you edit a software restriction policy, in the **Enforcement Properties** dialog box select **All software files except libraries (such as DLLs)** as shown in the following figure:

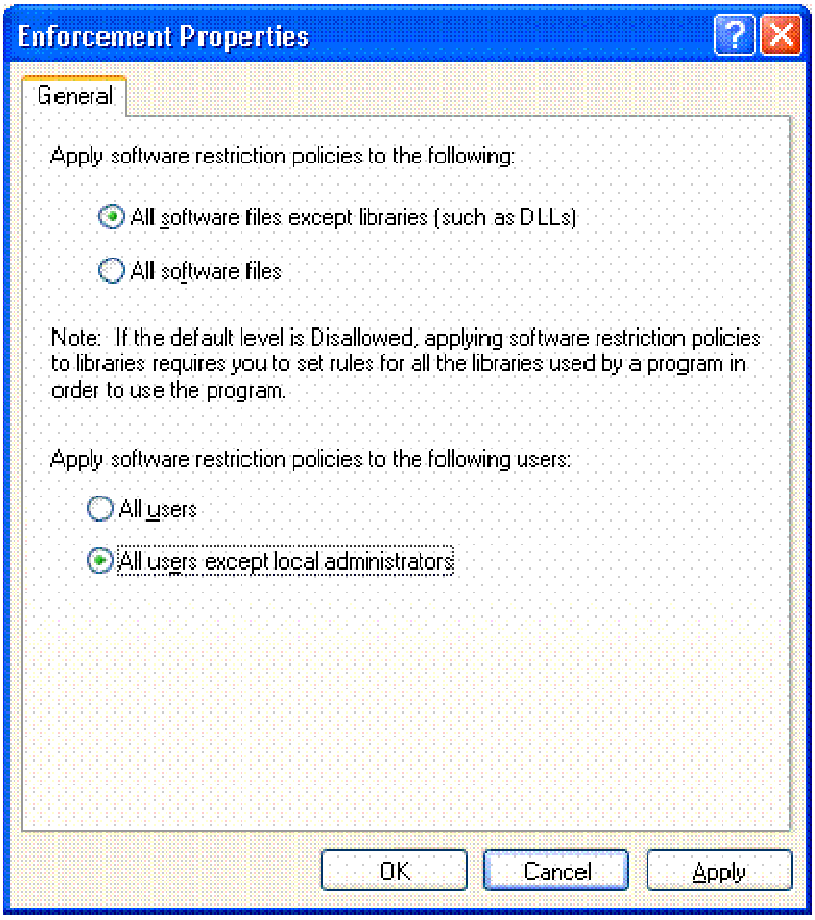


**Figure 6.8 The Enforcement Properties dialog box that shows file and user enforcement options**

# *Skip Administrators*

You may want to disallow programs from running for most users but allow administrators to run all of them. For example, an administrator may have a shared computer that multiple users connect to through Terminal Server. The administrator may want users to run only specific applications on the computer, but members in the local **Administrators** group to be able to run anything. Use the **Skip Administrators** enforcement option to achieve this functionality.

If the software restriction policy is created in a GPO that is linked to an object in Active Directory, Microsoft recommends that you deny the **Apply Group Policy** permission on the GPO to the **Administrators** group and not use the **Skip Administrators** option. This method consumes less network bandwidth because GPO settings that do not apply to administrators are not downloaded.

**Note**: Software restriction policy defined in local security policy objects cannot filter user groups, and would therefore require use of the **Skip Administrators** option.

**To turn on the Skip Administrators option**

- In the **Enforcement Properties** dialog box (shown in Figure 6.8), select **All users except local administrators**.

## Defining Executables

The **Designated File Types Properties** dialog box in the following figure lists the file types that are governed by software restriction policy. These file types are considered executable files. For example, a screen saver file (.scr), is considered an executable file because it loads as a program when you double-click it in Windows Explorer.

Software restriction policy rules only apply to the file types listed in the **Designated File Types Properties** dialog box. If your environment uses a file type that you want to apply rules to, add it to the list. For example, for Perl script files you may choose to add .pl and other file types associated with the Perl engine to the **Designated file types:** list under the **General** tab of the **Designated File Types Properties** dialog box.

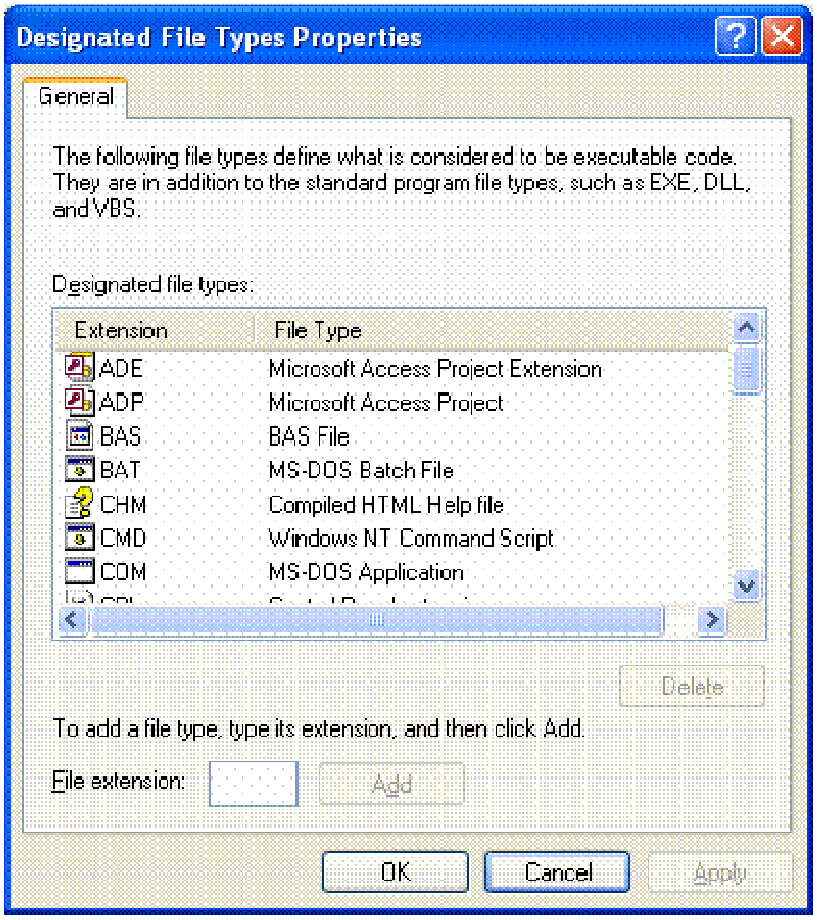


**Figure 6.9 The Designated File Types Properties dialog box**

For the GPO design that is defined in this guide, the file types .mdb and .lnk are removed and .ocx is added. The following table lists the designated file types.

**Table 6.2 Designated File Types**

| File extension | Description | File extension | Description |
|---|---|---|---|
| .ade | Microsoft Access Project extension | .msc | Microsoft Common Console document |
| .adp | Microsoft Access Project | .msi | Windows Installer Package |
| .bas | Visual Basic Class Module | .msp | Windows Installer Patch |
| .bat | Batch file | .mst | Visual Test Source file |
| .chm | Compiled HTML Help file | .ocx | ActiveX Control |
| .cmd | Windows NT command script | .pcd | Photo CD Image |
| .com | MS-DOS application | .pif | Shortcut to MS-DOS program |
| .cpl | Control Panel extension | .reg | Registry entry |
| .crt | Security certificate | .scr | Screen Saver |
| .exe | Application | .sct | Windows Script Component |
| .hlp | Windows Help file | .shs | Shell Scrap Object |
| .hta | HTML application | .url | Internet Shortcut (Uniform Resource Locator) |
| .inf | Setup Information file | .vb | Visual Basic file |
| .ins | Internet Communication setting | .vbe | VBScript Encoded Script file |
| .isp | Internet Communication setting | .vbs | VBScript Script file |
| .js | JScript file | .wsc | Windows Script Component |
| .jse | JScript Encoded Script file | .wsf | Windows Script file |
| .mde | Microsoft Access MDE Database | .wsh | Windows Scripting Host Setting file |

## Trusted Publishers

You can use the **Trusted Publishers Properties** dialog box to configure which users can select trusted publishers. You can also determine which, if any, certificate revocation checks are performed before you trust a publisher. With certificate rules enabled, software restriction policy will check a certificate revocation list (CRL) to ensure that the software's certificate and signature are valid. However, this process may decrease performance when signed programs are started.

The options on the **General** tab of the **Trusted Publishers Properties** dialog box shown in the following figure allow you to configure settings that are related to ActiveX controls and other signed content.

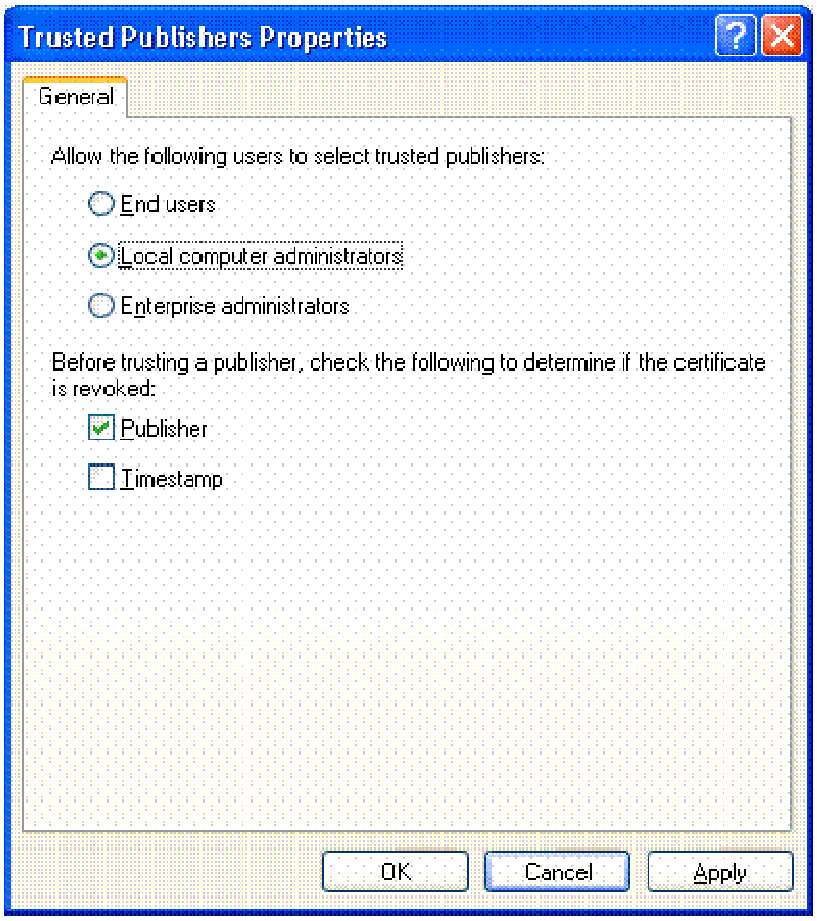


**Figure 6.10 The Trusted Publisher Properties dialog box**

The following table shows trusted publisher options that are related to ActiveX controls and other signed content.

**Table 6.3 Trusted Publisher Tasks and Settings**

| Setting name | Task |
|---|---|
| Enterprise administrators | Use to allow only enterprise administrators to make decisions about signed active content. |
| Local computer administrators | Use to allow local computer administrators to make all decisions about signed active content. |
| End users | Use to allow users to make decisions about signed active content. |
| Publisher | Use to ensure that the certificate the software publisher uses has not been revoked. |
| Timestamp | Use to ensure that the certificate the organization uses to time stamp the active content has not been revoked. |

# Software Restriction Policy Design and Deployment

This section describes how to administer software restriction policy with Group Policy snap-ins, things to consider when you edit a policy for the first time, and how to apply a software restriction policy to a group of users. A variety of issues that relate to software restriction policy deployment are also discussed.

## *Integration with Group Policy*

You can administer software restriction policy with Group Policy snap-ins to a set of client computers as well as to all the users that log on to the computers. The policy is applied to the Desktop OU and the Laptop OU that are defined in this guide.

### Domain

The administrator should create a separate GPO for the software restriction policy. This method provides a way to disable the Group Policy without disrupting other policies that are applied to the object if unexpected problems should arise.

### Local

A local policy should be configured for the stand-alone client computers in your environment as described in Chapter 5, "Securing Stand-Alone Windows XP Clients" of this guide.

## *Designing a Policy*

This section describes the steps to follow when you design and deploy a software restriction policy. Policy design requires you to make several decisions, all of which are described in the following table.

**Table 6.4 Important Policy Design Considerations**

| Decision | Factors to consider |
|---|---|
| Laptops or workstations | Investigate the needs of the mobile users in your environment to determine if the laptops require a different policy than that for desktops. Laptops tend to need more flexibility than desktops. |
| Server shares, logon scripts, and home drives | You will need to define a path rule for any applications that start from a server share or home directory. You can add logon script files to the path rule. If a script calls any other script, also add the executable locations to the path rule. |
| GPO or local security policy | In this guide a GPO is used for the design. However, you should consider the effects that local policy will have on your design. |
| User or computer policy | This design applies all settings at the computer level. |
| Default security level | It is recommended to configure the default setting to **Disallowed**, and then configure the rest of the policy accordingly. The **Unrestricted** default setting is also available. |
| Additional rules | You will need to apply additional operating system path rules as needed when you use the **Disallowed** default policy. In the **Disallowed** configuration, the four rules are created automatically. |

| Decision | Factors to consider |
|---|---|
| Policy options | If you use a local security policy and do not want the policy to apply to administrators on the client computers in your environment, select the policy enforcement option **Skip Administrators**.<br><br>If you want to check DLLs as well as executable files and scripts, select the policy enforcement option **DLL Checking**.<br><br>If you want to establish rules for file types that are not in the default list of designated file types, use the option to add them as needed to the **Designated File Types Properties** dialog box.<br><br>If you want to change who can make decisions about whether ActiveX controls and other signed content can be downloaded, select the check box for **Publisher** under the **General** tab of the **Trusted Publishers Properties** dialog box. |
| Applying the policy to a site, domain, or OU | The policy will reside under the OU in which the desktops and laptops are located. |

**Note**: Although this guide recommends that software restriction policy be enforced at the computer level there are many cases in which enforcement at the user level will make sense. For example, an organization with shared computers such as Terminal Server application servers or call center workstations may want to allow certain users to run a suite of applications, but block all other users from access.

## Best Practices

Microsoft recommends that you create a separate GPO for software restriction policy, so that if you need to disable the policy in an emergency it will not affect the rest of your domain or local policy.

Also, if you accidentally lock down a workstation with software restriction policy in the design phase of your OU, restart the computer in **Safe mode**, log on as a local administrator, and then modify the policy. Software restriction policy is not applied when you start Windows in **Safe mode**. After you start the computer in **Safe mode**, run Gpupdate.exe and then restart it.

For the best security, use ACLs in conjunction with software restriction policy and do not give users administrative privileges. Users may try to rename or move disallowed files or overwrite unrestricted files to circumvent software restriction policy. Use ACLs to deny users access to perform either of these actions. Users who are members of the local **Administrators** group will be able to bypass your software restriction policy implementation; therefore Microsoft recommends that you do not give users administrative privileges whenever feasible.

Login scripts are usually located under SYSVOL on the domain controller or a centralized server. The domain controller often changes with each login. If your default rule is set to **Disallowed**, be sure to create rules that identify the locations of your logon scripts. If the logon servers have similar names, consider the use of wildcards to locate them, or use the logon script name with unrestricted settings.

**Note**: Test new software restriction policy settings thoroughly in test environments before you apply them to your domain. New policy settings may act differently than originally expected. Thorough tests will diminish the chance that you will encounter a problem when you deploy the software restriction policy settings across your network.

# *Stepping Through the Process*

Use the following information to guide you through the process of software restriction policy design and application of the design as a GPO to the laptops and desktops in your environment.

## Step 1. Create a GPO for the OU

Locate the OU that was created for the desktops or laptops in your environment. If you are working on a stand-alone client computer, the policy settings are located in the Local Computer Policy. In this policy, click **Properties**, and then create a new GPO. Name the policy according to your organization's naming convention. Remember, this policy will only be used to enforce software restrictions.

## Step 2. Set the Software Restriction Policy

Highlight the GPO and click **Edit**. Traverse the tree until you locate **Windows Settings\Security Settings\Software Restriction Policy**. The first time you edit the policy you will see the following message:

> No Software Security Policies are defined.

This message warns you that you will define default values when you create a policy. These default values can override policy settings from other software restriction policies. Because no software restriction policy settings have been set yet, use the default settings to start. Right-click the **Actions** menu and select **New Software Restriction Policies**.

## Step 3. Set Up the Path Rules

After you determine which applications and scripts the workstations will use, you can set up the path rules. Some programs launch other programs to perform tasks, and the software applications in your environment may depend on one or more programs that support other programs. Inventory and installation documentation about the currently installed software is very useful for tracking path rules. An example of a workstation design might include the following guidelines:

- Applications = *\Program Files
- Shared Group Applications= g:\Group Applications
- Logon script = Logon.bat
- Desktop Shortcuts = *.lnk
- Approved VBS Scripts =*.vbs

## Step 4. Set the Policy Options

The following options include the recommended policy settings for the design that is defined in this guide. These options alter the enforcement behavior scope or the Authenticode trust settings for digitally signed files.

- **Enforcement**. If the computer is part of the domain, ensure that the **Domain Admins** group is automatically added to the **Administrators** group.
- **Apply to Users**. Includes all users except local Administrators. Use of this option delays the launch of each application. To compensate for this delay, the design configures the policy to not check DLLs.
- **Apply to Files**. Includes all software files except libraries (such as DLLs). Use of this option delays the launch of each application. To compensate for this delay, the design configures the policy to not check DLLs.

- **Designated file types**. For the GPO design that is defined in this guide, .ocx files were added to the list and .mdb and .lnk file types were removed. You could add custom application file type extensions as needed to make them subject to the same rules.
- **Trusted Publishers**. For the GPO design that is defined in this guide, the **Administrators** group was enabled and the option for **Trusted Publisher Properties: Local Computer Administrators** was selected.

Before you trust a publisher, select the **Check: Publisher** option when you design the GPO to ensure the policy will validate certificates.

## Step 5. Apply the Default Settings

It is a best practice to configure the policy to the default **Unrestricted** setting. This method ensures that the policy is properly initialized before software restrictions are applied. After you review the policy settings, reset the default setting to **Disallowed**.

## Step 6. Test the Policy

If the computer is part of a domain, move the computer into the OU container where the policy is applied. Restart the test computer and log on to it. The test plans should have instructions about how each of the applications should work when the policy is applied. Run the applications to ensure they have full functionality and that you can access all of their features. After you have validated the functionality of the applications, simulate an attack on the applications to ensure that the policy has no security vulnerabilities.

If the computer is a stand-alone client, log on to the test computer and follow your test plan. After you have validated the applications, launch the simulated attack again to ensure that the policy has no security vulnerabilities.

# *Deploying Software Restriction Policy*

After the policy is thoroughly tested, apply it to the desktop or laptop OU in your environment. If it is for a stand-alone client computer, apply it to the Local Computer Settings on the client. Open the MMC Computers and Users snap-in and traverse the directory until you reach the OU container for the desktops or laptops. Then, create the new GPO with the Group Policy Object Editor. Edit the properties and apply the appropriate policy settings based on the information in the following tables to the **Software Restriction Policy** under **Windows Settings\Security Settings**.

**Table 6.5 Security Levels**

| Default rule in UI | Description | Setting |
|---|---|---|
| Disallowed | Software will not run, regardless of the access rights of the user. | Use this default rule |

**Table 6.6 Additional Rules**

| Path rule | Setting |
|---|---|
| %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\SystemRoot% | Unrestricted |
| %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\SystemRoot%*.exe | Unrestricted |
| %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\SystemRoot%\System32*.exe | Unrestricted |

| Path rule | Setting |
|---|---|
| %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\ProgramFilesDir% | Unrestricted |
| *.vbs | Disallowed |
| G:\Group Applications | Unrestricted |
| Logon.bat or Logon script | Unrestricted |
| *\Program Files | Unrestricted |

**Table 6.7 Enforcement on Files and Users**

| Enforcement options | Recommendation |
|---|---|
| Apply software restriction policies to the following: | All software files except DLLs. |
| Apply software restriction policies to the following users: | All users except local administrators. |

**Table 6.8 Designated File Types**

| File types | Recommendation |
|---|---|
| Designated file types properties | Remove .mdb and .lnk file types and add .ocx. |

**Table 6.9 Trusted Publishers**

| Trusted publishers | Recommendation |
|---|---|
| Allow the following user groups to select trusted publishers: | **Local Computer Administrators** |
| Determine if the certificate is revoked. | Select the **Publisher** option. |

# Summary

Software restriction policy provides administrators with an effective way to identify and control software on computers that run Windows XP Professional. You can create policies to block malicious scripts, lock down computers in your environment in various ways, and prevent applications from running. In an enterprise organization, it is a best practice to manage software restriction policy with GPOs and to customize each policy to accommodate the needs of the different user groups and computers. Microsoft recommends that you not attempt to manage user groups in a stand-alone environment.

When correctly applied, software restriction policy will improve the integrity and manageability of computers in your organization and ultimately lower the ownership and maintenance costs of the operating systems on those computers.

# More Information

The following links provide additional information about Windows XP Professional security-related topics.

- For more information about software restriction policy, see "Using Software Restriction Policies to Protect Against Unauthorized Software" at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx.
- For more information about Group Policy, see "Windows Server 2003 Group Policy" at http://www.microsoft.com/windowsserver2003/technologies/management/grouppolicy/default.mspx.

# Chapter 7: Conclusion

Congratulations. Now that you have finished this guide, you should have a clearer understanding of how to assess risks that may affect the security of computers that run the Microsoft® Windows® XP Professional with Service Pack 2 (SP2) operating system in your organization. You have gained an understanding of how to plan for and design security into your infrastructure client computers where it is possible to do so.

This guide includes material from consultants and systems engineers who have implemented Windows XP, Microsoft Windows Server™ 2003, and Windows 2000 solutions in a variety of organizational settings. It is designed to provide you with a current set of best practices for working with Windows XP, and the prescriptive information in this guide can be applied to any organization.

Security is a serious topic, regardless of your organization's environment. However, many organizations do not emphasize security because they mistakenly view it as something that restricts their agility and flexibility. When well-designed security becomes a core business requirement and is planned for at the start of every information technology (IT) project, a properly implemented security strategy can help to improve the availability and performance of your computer systems. Conversely, a security strategy that is added to a project as an afterthought can negatively affect usability, stability, and management flexibility. For these reasons, this guide suggests that every organization consider security as one of its highest priorities.

## Securing the Client

Windows XP Professional offers a complete set of security solutions to safeguard against threats to desktop and laptop computers. Although users whose computers are not joined to a domain have fewer security options, both domain-joined and stand-alone users benefit from secure access to their computers.

### *Enterprise Clients*

When a client computer is part of an organization’s network, it is possible that the network administrator will configure the computer through the Group Policy security features of the Active Directory® directory service that are detailed in this guide. Any Group Policy settings that a network administrator applies take precedence over any local settings that users configure on their computers. Group Policy allows administrators to manage environments that include many different types of client computers.

### *Specialized Security – Limited Functionality Clients*

The Specialized Security – Limited Functionality (SSLF) environment that is described in this guide emphasizes the issues of access, services, and infrastructure environment. In addition to elevated security controls and user authentication, administrators have greater control over access to resources and objects on the network and the client workstations. This control is required by administrators who must keep data and resources secure, and will inevitably limit

what tasks can be performed on a SSLF client computer. However, this limited capability is necessary because of the increased security requirements in this type of environment.

### *Stand-Alone Clients*

Although fewer security policy settings are available for stand-alone client computers than those that belong to an Active Directory domain, key security features are available for such computers. Proper configuration of these policy settings on stand-alone computers will help minimize the risk of vulnerabilities being exploited. The stand-alone environment imposes more administrative overhead because these computers cannot be managed through domain-based Group Policy. However, use of the tools that are described in this guide will help to reduce administrative overhead.

## Software Restriction Policy

Software restriction policy provides administrators with a way to identify software that runs on client computers in a domain or stand-alone environment and control the software's ability to execute. It can be used to block malicious scripts or code and prevent the execution of unwanted applications. Software restriction policy can be configured for stand-alone systems or managed through domain-based Group Policy to promote improved system integrity and manageability.

## Summary

This guide explained how to effectively assess, prioritize, and mitigate security risks in three distinct environments for computers that run Windows XP with SP2. Documented methods about how to plan and design security for an organization's network infrastructure were provided, as well as detailed guidance about how to assess and mitigate specific vulnerabilities on computers in the types of environments that are defined in the guide.

The reasons for the choices that were made are explained in terms of the tradeoffs that are involved when an organization decides whether to implement the different policy settings for the three environments. Detailed information is provided about how specific policy settings may affect functionality, manageability, performance, and reliability so that you can make informed choices about which settings to implement in your own environment.

It is important to understand that the task of securing the client computers in your network is not a one-time project but a continuous process. Organizations should include security-related tasks and planning in their budgets and schedules. Implementation of every policy setting that is discussed in this guide will improve the security in most organizations that operate Windows XP Professional. However, when the next serious vulnerability is discovered, these environments may again be susceptible to attack. For this reason, it is critical to monitor a variety of resources to stay current about security issues that are related to the operating systems, applications, and devices in your environment.

Every member of the team that produced this guide hopes that you find the material in it to be useful, informative, and easy to understand.

# More Information

The following links provide additional information about Windows XP Professional security-related topics.

- For links to common questions and answers, instructions, the latest downloads, and more, see the Windows XP Help and Support at http://support.microsoft.com/winxp.
- For information about maintaining security with Windows XP, see the Trustworthy Computing: Security site at http://www.microsoft.com/mscorp/twc/security/default.mspx.
- For information about security on TechNet, see the Technet Security Center at http://www.microsoft.com/technet/security/default.mspx.
- For information about planning for Windows XP Professional, see the Windows XP Professional – Plan page on TechNet at http://www.microsoft.com/technet/prodtechnol/winxppro/plan/default.mspx.
- For Security How-to Resources for Windows XP Professional, see http://www.microsoft.com/technet/itsolutions/howto/sechow.mspx.
- For how-to information about Encrypting and Decrypting Data with the Encrypting File System (EFS), see http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_seconceptsunencrypt.mspx.

# Appendix A: Key Settings to Consider

Although this guide discussed many security countermeasures and security settings, it is important to understand that some of them are especially important. This appendix highlights those settings; you may wish to refer to the relevant chapter for an explanation of what the setting does and why it is important.

The settings that should be included in this list could be debated extensively. In fact, this topic was discussed at great length by a group of security experts within Microsoft. You may feel that some settings are missing, or that some of the listed settings do not need to be on the list. Because each organization has a distinct environment with unique business requirements, different opinions about security issues should be expected. Nevertheless, this list might help you prioritize tasks that are related to hardening computers that run Microsoft® Windows®.

## Important Countermeasures

Important countermeasures that are not related to security settings include:

- Keep computers up-to-date on service packs and hotfixes with automated tools for testing and deployment.
- Install and configure distributed firewall software or organizational IPsec policies.
- Deploy and maintain antivirus software.
- Deploy and maintain antispyware software.
- Use an unprivileged account for day-to-day tasks. You should only use an account with administrator privileges to perform tasks that require elevated privileges.

## Key Security Settings

Key security settings that are available in Microsoft Windows include the following:

- Password policy settings, which are discussed in Chapter 2, "Configuring the Active Directory Domain Infrastructure:"
    - Enforce Password History
    - Maximum Password Age
    - Minimum Password Length
    - Passwords must meet complexity requirements
    - Store Password Using reversible encryption for all users in the domain

- User rights assignment settings, which are discussed in Chapter 3, "Security Settings for Windows XP Clients:"
  - Access this computer from the network
  - Act as part of the operating system
  - Allow logon locally
  - Allow Log on through Terminal Services
- Security option settings, which are discussed in Chapter 3, "Security Settings for Windows XP Clients:"
  - Accounts: Limit local account use of blank passwords to console logon only
  - Domain Member: Digitally encrypt or sign Secure channel Data (always)
  - Domain Member: Digitally encrypt Secure channel Data (when possible)
  - Domain Member: Digitally sign Secure channel Data (when possible)
  - Domain member: require strong (windows 2000 or later) session key
  - Network access: Allow anonymous SID/Name translation
  - Network Access: Do not allow anonymous enumeration of SAM accounts
  - Network access: do not allow enumeration of SAM accounts and shares
  - Network Access: Let Everyone permissions apply to anonymous users
  - Network Access: Remotely Accessible Registry Paths
  - Network Access: Restrict Anonymous access to named pipes and shares
  - Network Access: Shares that can be accessed anonymously
  - Network Access: Sharing and Security Model for Local Accounts
  - Network Security: Do not store LAN manager hash value on next password change
  - Network Security: LAN Manager Authentication Level
- Additional registry settings, which are discussed in Chapter 3, "Security Settings for Windows XP Clients," especially the following setting:
  - Safe DLL Search Mode

# Appendix B: Testing the Windows XP Security Guide

## Introduction

The function of the *Windows XP Security Guide* is to provide proven and repeatable configuration guidance to secure computers that run Microsoft® Windows® XP Professional with Service Pack 2 (SP2) in a variety of environments.

The *Windows XP Security Guide* was tested in a lab environment to ensure that the guidance works as expected. The documentation was checked for consistency and all recommended procedures were tested by the *Windows XP Security Guide* test team. Tests were performed to verify functionality, but also to help users of the guidance to reduce the amount of resources that are needed to build and test their own implementations of the solution.

### *Scope*

The *Windows XP Security Guide* was tested in a lab environment for two different security environments—Enterprise Client (EC) and Specialized Security – Limited Functionality (SSLF). These environments are described in Chapter 2, "Configuring the Active Directory Domain Infrastructure." Tests were conducted based on the criteria that are described in the following "Test Objectives" section.

A vulnerability assessment of the test lab environment that was used to secure the *Windows XP Security Guide* solution was out of scope for the test team. Penetration testing was performed by partners.

### *Test Objectives*

The *Windows XP Security Guide* test team was guided by the following test objectives:

- Ensure that the prescriptive configuration and policy settings for Windows XP Professional with SP2 interoperate correctly and as expected in a Windows Server™ 2003–based domain network for the two different security environments.
- Ensure that Windows XP Professional SP2 client computers are able to perform the basic tasks and applications that are listed in the included test cases.
- Verify that all prescriptive guidance in version 2.1 of the *Windows XP Security Guide* is clear, complete and technically correct.
- Verify that the security templates work as expected on the Windows XP Professional SP2 client operating system.
- Verify that the Administrative Templates and Software Restriction Policy recommendations work as expected on the Windows XP Professional SP2 client operating system.

Finally, the guidance should be repeatable and reliably usable by a Microsoft Certified Systems Engineer (MSCE) with two years of experience.

# Test Environment

The test environment consisted of a Windows Server 2003 SP1 Active Directory® directory service, computers for infrastructure server roles that provided domain controller, DNS, and DHCP services, and other computers for application server roles that provided file, print, Web, CA, and Microsoft Exchange 2003 e-mail services. The desktop and laptop client computers in the domain used Windows XP Professional with SP2.

The network also contained two client computers that used Windows XP Professional with SP2 in workgroup mode that were used to test stand-alone security templates. Laptop computers in the domain network were reused to test stand-alone laptop security templates. The following figure illustrates the test network.

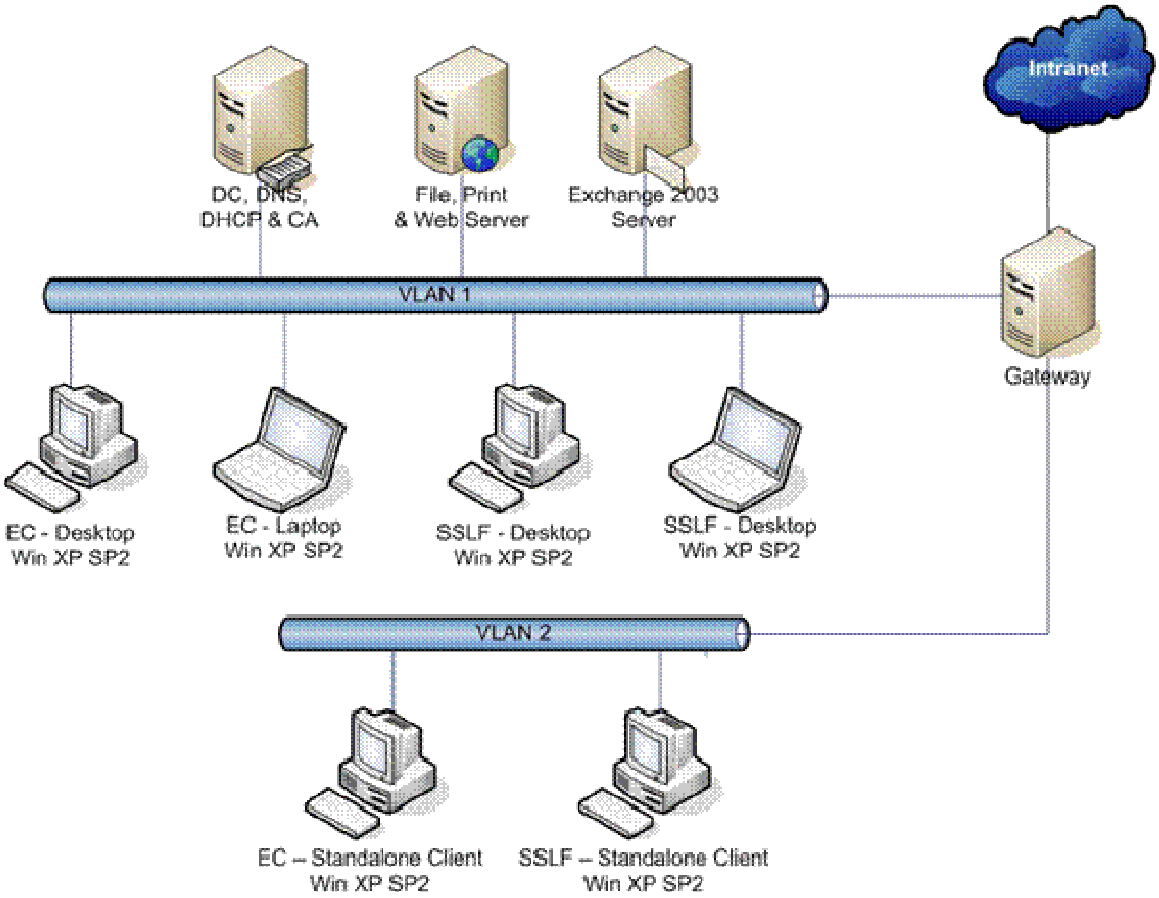


**Figure B.1 The network that was used to test the *Windows XP Security Guide* in domain and stand-alone mode**

The network in the following figure was developed to test the legacy templates that are included with this guide.

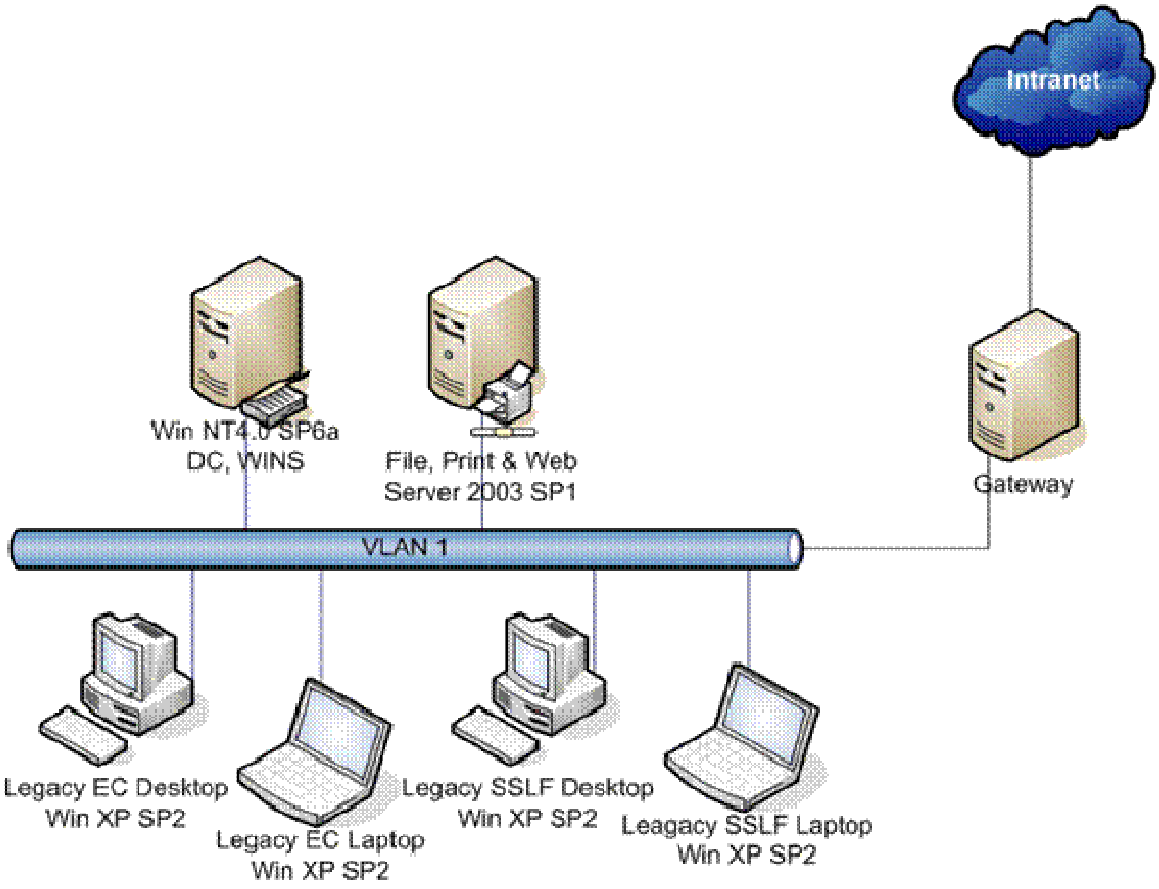


**Figure B.2 The network that was used to test the legacy security templates that are included with this guide**

# Testing Methodology

This section describes the procedures that were followed to test the *Windows XP Security Guide*.

The test team established a lab that incorporated the networks that are illustrated in the previous section. The test team executed a quick proof of concept (POC) test pass and then two more robust test cycles. During each pass the team strove to stabilize the solution.

A test cycle was defined as a sequence of the following two incremental build phases:

1. Manual computer configuration phase
2. Group/Local Policy configuration phase

The details of each phase are provided in the following "Phases in a Test Pass" section. The "Test Preparation Phase" section describes the steps that were performed to ensure that the lab environment was free of any issues that could cause a misinterpretation of the actual test results after both of the environment scenarios were hardened through the two incremental build phases.

In each test pass, different sets of test cases were executed. These tests are explained in the "Types of Tests" section later in this appendix.

# *Phases in a Test Pass*

This solution was tested in the phases that are described in the following subsections. Any critical issues that were found in a build phase were raised as bugs and resolved in that phase before the test team moved to the next incremental phase. This method ensured that critical issues were resolved quickly. It also minimized the need for resources that would be needed to debug issues that were found in later phases.

## Test Preparation Phase

This phase set up the baseline network to which the solution was applied. It consisted of the following steps.

**To perform the test preparation phase**

1. Network the computers as illustrated in the network diagram and install the appropriate versions of the Windows operating system on all server and client computers.
2. Create and configure domain controllers, domains, and each server role. Join the Windows XP Professional with SP2 client computers to the domain.
3. Install user applications on each of the Windows XP Professional with SP2 client computers.
4. Execute basic verification tests to confirm proper network configuration. Ensure client computer accessibility to the services that are provided by the domain controller and member servers (DNS, DHCP, CA, file, print, Web and e-mail).
5. Execute the installed applications to verify that there are no installation problems and that all the applications run properly.
6. Check the event log to ensure that there are no errors.
7. After the previous steps are completed, create an image backup of each computer. These backup images are used to "roll back" the network to the default state before a new test pass is started.

## Manual Configuration Phase

This phase is often the first security build phase. It consists of the following build procedure.

**To perform the manual configuration phase**

1. The Microsoft Management Console (MMC) Computer Management snap-in is used to perform the prescribed policy setting changes, such as the local administrator account and password on each member computer. Complete the following steps to secure the domain accounts (Guest and Administrator accounts):
    a. Disable the Guest account.
    b. Ensure that the built-in Administrator account has a complex password, has been renamed, and has had its default account description removed.
    c. Incorporate any additional recommendations from the guide about how to secure the domain accounts.
2. Perform all other applicable manual hardening procedures as prescribed in each chapter of the guide.
3. For stand-alone Windows XP client computers, manually create a secure database.

## Group/Local Policy Configuration Phase

In this phase, the Group Policy objects (GPOs) are applied at the domain and organizational unit (OU) levels. GPOs are applied to the different OUs based on the recommendations in Chapter 2, "Configuring the Active Directory Domain Infrastructure." For stand-alone Windows XP client computers, local policy is configured. This phase consists of the following steps.

**To perform the Group/Local Policy configuration phase**

1. Create the described OU structure to support Group Policy recommendations that are made in the guide.
2. Move the Windows XP desktop and laptop client computers to the appropriate OUs.
3. Identify the domain users and move them to the appropriate OUs so that you can apply the Administrative Templates.
4. Add a new GPO link for each OU.

   **Note**: You might need to elevate the GPO links in the priority list where default GPO links are already present.
5. Import the security template that was included with the guide into the GPO.
6. For each environment scenario in the different chapters, apply the appropriate Group Policy on each OU.

# *Test Execution Details*

Chapters 2 through 6 of the *Windows XP Security Guide* provide instructions for applying the security recommendations to the domain, Windows XP desktop computers, Windows XP laptop computers, and Windows XP stand-alone client computers for the Enterprise Client (EC) and Specialized Security – Limited Functionality (SSLF) environments that are defined in the guide. These recommendations are accompanied by a Microsoft Excel® workbook, security templates, Administrative Templates and automated scripts. The automated scripts are used to import templates into the local GPO on the secure stand-alone client computers. This section explains how the recommendations were implemented and tested.

## Chapter 2: Configuring the Active Directory Domain Infrastructure

Complete the following procedures to test this chapter.

**To verify the baseline network**

- Complete the basic verification test cases to ensure that the image backups function properly. A successful completion of these test cases confirms that the entry criteria are met.

**To start the manual configuration phase**

1. Synchronize the time of all the domain member servers and the Windows XP client computers with the domain controller.
2. Disable the Guest account.
3. Rename the Administrator and Guest accounts.
4. Change the Administrator password.

**To implement the OU structure configuration**

1. In the corp.woodgrovebank.com domain, create an OU with the name "Department OU."
2. Create two sub-OUs in the Department OU. Name them "Windows XP OU" and "Secured XP Users OU."
3. In the Windows XP OU, create the following four sub-OUs:
   - EC Desktop OU
   - EC Laptop OU
   - SSLF Desktop OU
   - SSLF Laptop OU
4. Move the Windows XP computers that are assigned to each security environment to their respective OUs.
5. Move the domain users that will log on to the Windows XP client computers to the Secured XP Users OU.
6. Create and link a new GPO with the name "Domain Policy" on the corp.woodgrovebank.com object. Click **Up** on the Group Policy tab of domain object in the MMC Active Directory Users and Computers snap-in to ensure the highest priority for the new GPO, and then import the appropriate security template (SSLF-domain.inf or EC-domain.inf) into the GPO.
7. Execute **gpupdate /force** on the domain controller to download the latest Group Policy settings.

# Chapter 3: Security Settings for Windows XP Clients

This chapter describes the primary settings that are configured through Group Policy in a Windows Server 2003 domain. The chapter prescribes policy settings for the two defined security environments to ensure that Windows XP with SP2 desktops and laptops are secure.

**To configure the security template settings**

1. Execute the base deployment tests to verify that all the recommendations in the guide are appropriate for your environment. Review the recommended policy settings. Modify the settings in the security templates as needed before you proceed to deploy them.
2. Link new GPOs to each of the two Desktop OUs. For the Enterprise Client environment, import the EC-desktop.inf security template into the GPO. For the Specialized Security – Limited Functionality environment, import the SSLF-desktop.inf security template into the GPO.
3. Link new GPOs to each of the two Laptop OUs. For the Enterprise Client environment, import the EC-Laptop.inf security template into the GPO. For the Specialized Security – Limited Functionality environment, import the SSLF-Laptop.inf security template into the GPO.
4. Log on to a Windows XP client computer and execute the **gpupdate /force** command. Then restart the computer to ensure that the latest Group Policy settings are downloaded.
5. Run the tests that are listed later in this document.

# Chapter 4: Administrative Templates for Windows XP

This chapter describes how to configure and apply additional policy settings on computers that run Microsoft Windows XP with SP2 by using Administrative Templates.

**To configure the Administrative Template settings**

1. Execute the base deployment tests to verify that all the recommendations in the guide are appropriate for your environment. Review the recommended policy settings. Modify the settings in the Administrative Templates as needed before you proceed to deploy them.
2. Create four new GPOs, one for each of the four types of Windows XP client computers. Because there is some variation in the policy settings for desktops and laptops, it is suggested that you create separate GPOs for each.
   - EC Desktop Administrative Template Policy
   - EC Laptop Administrative Template Policy
   - SSLF Desktop Administrative Template Policy
   - SSLF Laptop Administrative Template Policy
3. In the Administrative Templates, configure the computer configuration settings and the user configuration settings for each of the GPOs according to the guidance that is provided in Chapter 4, "Administrative Templates for Windows XP."
4. Link the GPOs to their respective OUs.
5. Log on to a Windows XP client computer and execute the **gpupdate** /**force** command. Then restart the computer to ensure that the latest Group Policy settings are downloaded.
6. Run the tests that are listed later in this appendix.

# Chapter 5: Securing Stand-Alone Windows XP Clients

This chapter describes the primary policy settings that are set through local computer policy. The prescribed setting values will help ensure that stand-alone desktops and laptops in the organization that run Windows XP with SP2 are secure.

**To configure security settings on stand-alone Windows XP clients**

1. Execute the base deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Use the MMC Security Configuration and Analysis snap-in to create a security database. This database will be used to write to local policy. Step-by-step guidance is provided in Chapter 5, "Securing Stand-Alone Windows XP Clients."
3. Use the Security Configuration and Analysis snap-in to apply the policy settings that are included in the stand-alone security template files. Step-by-step guidance is provided in Chapter 5, "Securing Stand-Alone Windows XP Clients." It is important to use the Security Configuration and Analysis snap-in, because system services policy settings cannot be applied with the Local Computer Policy snap-in.
4. Run the appropriate automated script (included with this guide) to import the security templates.
5. Run the tests that are listed later in this appendix.

## Chapter 6: Software Restriction Policy for Windows XP Clients

This chapter allows administrators to identify and control the software that runs in their domain. The tool that is used to accomplish this control is a policy-driven mechanism called software restriction policy.

**To configure software restriction policy**

1. Execute the base deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Locate the OU that was created for the Windows XP desktops and laptops. For stand-alone client computers, the policy settings are located in the local security policy. Create a new GPO for the Windows XP OU. Remember, this new GPO is only used for the software restriction policy.
3. Configure the software restriction policy as follows:
   a. Create a default software restriction policy.
   b. Set up the path rules.
   c. Set the policy options, such as enforcement, designated file types, and trusted publishers according to the prescriptions that are provided.
4. Review the policy settings and then reset the default policy setting to **Disallowed**.
5. Log on to a Windows XP client computer and execute the **gpupdate** /**force** command. Then restart the computer to ensure that the latest Group Policy settings are downloaded.
6. Run the tests that are listed later in this appendix.

## Verifying Group Policy Download on the XP Client

In the previous sections, GPOs were applied to OUs, which then applied the GPOs to the computers in the OUs. Complete the following steps to confirm the successful download of Group Policy from the domain controller to a Windows XP client computer. It is assumed that the client computer was restarted after the GPO was linked to the OU.

**To verify Group Policy download on a Windows XP client computer**

1. Log on to the Windows XP client computer.
2. Click **Start**, **Run**, type **rsop.msc**, and press ENTER.
3. In the **Resultant Set of Policy** console, expand **Console Root** and browse to **Computer Configuration**.
4. Right-click **Computer Configuration** and click **Properties**.

   The list of GPOs will display in the **Computer Configuration Properties** panel. The GPO that was applied to the OU should be available in the list, and there should be no errors associated with it.
5. Verify the Administrative Templates policy settings.

   Only the settings that are configured in the Administrative Template GPO should be visible in the respective **Administrative Templates** folder tree under **Computer Configuration** or **User Configuration**.

# *Types of Tests*

The test team performed the following types of tests during the testing phases to ensure that the secured Windows XP client computers are able to perform basic tasks without significant loss of functionality. You may want to refer to the Excel workbook "Windows XP Security Guide Test

Cases.xls," which is in the **Windows XP Security Guide Tools and Templates****Test Tools** folder that is included in the download for this guide. This workbook file contains the complete list of test cases that were executed for domain–based XP client computers and stand-alone XP client computers, as well as details such as test scenarios, execution steps, and expected results.

## Application Tests

These tests check whether user applications that are installed on the Windows XP client computers (such as the Office 2003 application suite, Windows Media® Player, and a few more) work properly. For more details about the test cases, refer to the Microsoft Excel workbook Windows XP Security Guide Test Cases.xls that is included with this guide.

## Automated Script Tests

Some of the test case scenarios were scripted in VBScript. These test cases are primarily concerned with proper functionality of Windows XP client computers that use network–based services, such as domain logon, password change, and print server access. The VBScript files for these test cases are available in the **Windows XP Security Guide Tools and Templates****Test Tools** folder that is included in the download for this guide.

## Basic Verification Tests

These test cases are a subset of the Application, Automated Script and Internet tests. They are basic tests that cover a variety of different scenarios, such as the ability to run applications that are installed on the client, client-server communication tests, the ability to access the Internet and download patches, and tests that monitor errors on the host. These test cases are also executed when you establish a baseline for the network during the Test Preparation phase.

## Documentation Build Tests

These tests validate that the statements, procedures, and functions that are documented in the implementation guidance are accurate, unambiguous, and complete. No separate test cases are listed for these tests.

## Functional Tests

These tests are designed to verify that the system that was built from the build guidance works correctly and as expected. They verify the functionality, health, and effect of the build procedures on the desktop and laptop client computers.

## Internet–Based Tests

Today's computer users typically need to access the Internet. These test cases ensure that some of the common day-to-day capabilities (browse to Web sites, use the Windows Messenger service, and download critical updates from the Microsoft Update site) are not affected by the lockdown of the Windows XP client computer.

# Pass and Fail Criteria

Before tests were performed, the following criteria were defined to ensure defect prevention and bug resolution:

- All test cases must pass with expected results as described in the individual test case spreadsheets.
- A test case is considered to have passed if the actual result matched the expected result that is documented for the case. If the actual result does not match the expected result, it was treated as a failed test case, a bug was created, and a severity score assigned.
- If a test case failed, it was not assumed that the solution guidance was necessarily defective. For example, misinterpretation of product documentation, incomplete documentation, or inaccurate documentation could cause failures. Each failure was analyzed to discover its cause based on actual results and the results that were described in project documentation. Failures were also escalated to the appropriate owners of the respective Microsoft products.

# Release Criteria

The primary release criterion for the *Windows XP Security Guide* was related to the severity of bugs that were still open. However, other issues that were not being tracked through bugs were also discussed. The criteria for release are:

- No bugs are open with severity levels 1 and 2.
- All open bugs are triaged by the leadership team, and their impacts are fully understood.
- Solution guides are free of comments and revision marks.
- The solution successfully passes all test cases in the test lab environment.
- Solution contents have no conflicting statements.

# Bug Classification

The bug severity scale is described in the following table. The scale is from 1 to 4, with 1 as the highest severity and 4 as the lowest severity.

**Table B.1 Bug Severity Classification**

| Severity | Most common types | Conditions required |
|---|---|---|
| 1 | – Bug blocked build or further testing.<br>– Bug caused unexpected user accessibility.<br>– Steps defined in the documentation were not clear.<br>– Results or behavior of a function or process contradicts expected results (as documented in functional specification).<br>– Major mismatch between the security template files and the functional specification. | – Solution did not work.<br>– User could not begin to use significant parts of the system.<br>– User had access privileges that should not be allowed.<br>– User access was blocked to certain server(s) that should be allowed.<br>– Expected results were not achieved.<br>– Testing cannot proceed without being addressed. |
| 2 | – Steps defined in the guide are not clear.<br>– Documented functionality is missing (in this case, test was blocked).<br>– Documentation is missing or inadequate.<br>– Inconsistency between security template files and content in the guide, but security template file is in sync with functional specification. | – User had no simple workaround to amend the situation.<br>– User could not easily figure out a workaround.<br>– Primary business requirements could not be met by the system. |
| 3 | – Documented format issue.<br>– Minor documentation errors and inaccuracies.<br>– Text misspellings. | – User has a simple workaround to mend situation.<br>– User can easily figure out workaround.<br>– Bug does not cause a bad user experience.<br>– Primary business requirements are still functional. |
| 4 | – Suggestions.<br>– Future enhancements. | – Clearly not related to this version. |

# Summary

This document enables an organization that implements the *Windows XP Security Guide* to understand the procedures and steps that were used to test the implementation of the solution in a test lab environment. The actual experience of the *Windows XP Security Guide* test team is captured in this document, which includes descriptions of the test environment, types of tests, the release criteria, and bug classification details.

All of the test cases that were executed by the test team passed with the expected results. The test team confirmed that the requisite functionality was available after the recommendations from the *Windows XP Security Guide* for the defined environments were applied.

# Acknowledgments

The Microsoft Solutions for Security and Compliance group (MSSC) would like to acknowledge and thank the team that produced the *Windows XP Security Guide*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

## Authors

Steve Clark

Mike Danseglio

Kurt Dillard

Richard Harrison, *Content Master*

Steve Ryan, *Content Master*

Jose Maldonado

Bob Partridge

Tony Quinn

## Program Managers

Bomani Siwatu

Alison Woolford, *Content Master*

## Release Managers

Flicka Crandell

Karl Seng, *Siemens Agency Services*

## Testers

Paresh Gujar, *Infosys Technologies*

Ashish Java, *Infosys Technologies*

Mehul Mediwala, *Infosys Technologies*

Rob Pike

Varun Rastogi, *Infosys Technologies*

Avrojit Ray, Infosys Technologies

## Editors

Reid Bannecker, *Volt Information Sciences*

John Cobb, *Volt Information Sciences*

Kelly McMahon, *Content Master*

John Tobey, *Volt Information Sciences*

Steve Wacker*, Wadeware LLC*

## Reviewers

Roger Abell, *Arizona State University*

Rich Benack

Shelly Bird

Susan Bradley

Duane Crider

Steve Dodson

Christine Duell

Mike Kaczmarek

Mark Kradel

Mike Lonergan

James Noyce, *Business Critical Consulting*

Joe Porter

Tom Shinder

Ben Smith

Josh Vincent

Jessica Zahn

Jim Whitney, *Configuresoft*

Jeff Williams

## Contributors

Ignacio Avellaneda

Tony Bailey

Ganesh Balakrishnan

Nathan Buggia

Derick Campbell

Chase Carpenter

Bryan Chee

Jeff Cohen

Mike Danseglio

John Dwyer

Sean Finnegan

Jose Maldonado

Karl Grunwald

Jesper Johansson

Joanne Kennedy

Karina Larson, *Volt Information Sciences*

Chrissy Lewis, *Siemens Business Services*

Frank Manning, *Volt Information Sciences*

David Mowers

Jeff Newfeld

Rob Oikawa

Bill Reid

Stacey Tsurusaki, *Volt Information Sciences*

David Visintainer *Volt Information Sciences*

Jay Zhang

At the request of Microsoft, the Center for Internet Security (CIS) and the United States Department of Commerce National Institute of Standards and Technology (NIST) participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.